М.А. СОКОЛОВА

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ – ОСНОВА ЦИФРОВОГО ДОВЕРИЯ

МАТЕРИАЛЫ ДЛЯ ОБСУЖДЕНИЯ

Минск, 2014

ОГЛАВЛЕНИЕ

Оглавление

АННОТАЦИЯ

Аннотация

Цель данного документа заключается в инициировании дискуссии по двум принципиальным вопросам, которые в значительной степени определяют позиции в отношении политики защиты персональных данных: права субъектов персональных данных и ответственность организаций (государственных и коммерческих), использующих эти данные.

Из всего комплекса взаимосвязанных проблем акцент сделан, прежде всего, на балансе приватности и безопасности (раздел «Что угрожает цифровому доверию?», «Защита персональных данных: между приватностью и безопасностью»). В разделе «В чём суть проблемы?» инструменты защиты прав субъектов персональных данных и акторы, которые связывают свои решения с регулированием в этой сфере, охарактеризованы на основании анализа и международного опыта. В разделе «Защита персональных данных в Беларуси» проблема структурирована по трем параметрам: содержание понятий, инструменты, акторы.

В выводах предлагаются обобщенные рекомендации относительно возможных направлений деятельности и тематики общественных дискуссий.

Регулирование защиты персональных данных в Беларуси представляет собой фрагментированный набор норм и правил, которые во многих случаях не соответствуют международным стандартам и не обеспечивают надлежащей защиты качества данных и прав субъектов данных. Поэтому очевидна необходимость:

- разработки единой стратегии, концепции или кодекса защиты персональных данных,
- создания единого экспертного органа по защите прав субъектов персональных данных,
- расширения репертуара инструментов политики (в том числе поощрение саморегулирования, принятие закона о саморегулировании),
- введения обязательной оценки влияния на приватность,
- гармонизации беларусского законодательства с международными принципами и нормами,
- повышения ответственности органов государственного управления и бизнеса.

Закон – самый важный инструмент регулирования, но он должен быть гибким. Принципы закона должны быть специфицированы в других инструментах.

Разработка политики в отношении персональных данных и внедрение стандартов и правил должны проходить в режиме консультаций с представителями бизнеса, общественных организаций и технического сообщества.

Ключевым условием такого диалога является просвещение и повышение осведомленности, как граждан – «субъектов персональных данных», так и распорядителей данных (государственных органов и коммерческих организаций).

АННОТАЦИЯ

Диалог всех заинтересованных сторон о способах реформирования существующего в Беларуси режима политики в отношении защиты персональных данных может фокусироваться на следующих вопросах:

- наборе основополагающих принципов защиты персональных данных,
- рационализации и усовершенствовании подходов к регулированию защиты персональных данных с учетом
  - приоритета защиты граждан как стороны, обладающей наименьшими возможностями по защите своих персональных данных при взаимодействии с бизнесом и государством,
  - важности поддержки саморегулирования и рыночных механизмов,
  - минимизации препятствий добросовестной коммерческой деятельности,
- прозрачности деятельности органов государственной власти.

Введение

Экспоненциальный рост объема данных изменяет мир значительнее, чем мы это представляем. Широкое распространение и применение информационных технологий обеспечивают гражданам реализацию одного из главных демократических прав на свободу информации, а ведение масштабных автоматизированных баз данных не только существенно оптимизирует процессы принятия решений, но и облегчает гражданам доступ к услугам цифрового рынка – от использования кредитных карт до формирования биометрического портрета и прогнозирования возможных заболеваний.

Вместе с тем активное использование персональных данных органами государственной власти, коммерческими и общественными организациями существенно усиливает риск несанкционированного вторжения посторонних лиц в частную жизнь, создает угрозу нарушения одного из его основополагающих естественных прав – права на неприкосновенность частной жизни. Особым институтом права на неприкосновенность частной жизни в условиях автоматизации и развития новых информационных технологий является институт персональных данных – любой информации, относящейся к прямо или косвенно определенному либо определяемому физическому лицу (субъекту персональных данных). Гарантия права на защиту таких данных – основа обеспечения приватности в информационной сфере.

Персональные данные -любая информация, относящаяся к прямо или косвенно определенному либо определяемому физическому лицу (субъекту персональных данных

В мире тесных экономических взаимосвязей отдельные наборы данных больше нельзя рассматривать изолированно. В условиях, когда данные могут храниться на протяжении длительного времени, «поступки» подростка, совершенные онлайн, могут оказать влияние на его профессиональную карьеру через много лет. Граждане все яснее понимают, что за ними постоянно «следят» государственные органы и частные организации. Это вызывает недоверие, как к тем, так и к другим.

Для того, чтобы граждане и потребители доверяли органам государственного управления, частному бизнесу и юридическим лицам нужны определенные меры защиты данных. Именно безопасность использования данных и гарантия соблюдения

прав субъектов персональных данных – основа «цифрового доверия», доверия организациям (государственным и частным), доверия технологиям, доверия людям.

Безопасность использования данных и гарантия соблюдения прав субъектов персональных данных – основа «цифрового доверия»: доверия организациям (государственным и частным), доверия технологиям, доверия

В большинстве стран обеспечение автономии индивида, его права контролировать использование информации о себе признаются основными принципами политики в отношении персональных данных. Однако проблема баланса ценностей остается нерешенной.

Дискуссии о защите персональных данных и неприкосновенности частной жизни уже стали частью нашей повседневности.

Анализ международных и национальных дискуссий позволяет определить координаты формирования позиций следующим образом:

1. Обеспечение надлежащего баланса между защитой информации о личности и требованиями свободного обмена информацией, свободы слова, свободы доступа к информации.
2. Граница вторжения в частную жизнь в интересах безопасности, в том числе национальной.
3. Синхронизация новых технологий и организационных практик, их влияния на защиту персональных данных. Такая политика должна быть не реактивной (непосредственная реакция на очевидные вызовы «сегодняшнего дня»), а проективной – технологически нейтральной и теоретически осмысленной.
4. Ценность информационной приватности:
   - неприкосновенность цифровой сферы частной жизни индивида может рассматриваться либо как фундаментальная ценность, либо как инструментальная, обеспечение которой необходимо в целях защиты других прав индивидов или благосостояния общества;
   - защита персональных данных может рассматриваться как единый комплекс (объект) регулирования или как совокупность проблем, каждая из которых регулируется в рамках различных законов, норм и правил (контекстуальная неприкосновенность)[1]. Отсюда, естественно, возникает вопрос: следует ли

[1] Schoeman, D. (1984) Philosophical Dimensions of Privacy: An Anthology. Доступно через: http://books.google.by/books/about/Philosophical_Dimensions_of_Privacy.html?id=q_FrmXyl3hUC&redir_esc=y

Аргументированное решение задачи защиты персональных данных – это всегда непростой процесс анализа последствий с учетом интересов различных сторон в конкретной ситуации. При этом никакое решение не может быть окончательным. А широкое общественное обсуждение должно стать гарантией того, что новые вызовы и возможности ответов на них в достаточной степени учитываются при разработке стратегий.

(Ч. Рааб)

вообще вырабатывать какую-то единую политику по отношению к защите персональных данных?

5. Выбор позиции относительно международных инструментов регулирования защиты персональных данных и методов:

- формирование «мирового порядка защиты персональных данных» на основе требований пересмотренной директивы Европейского Союза,
- создание международного надзорного органа,[1]
- выбор форм реализации международных норм на национальном уровне.

6. Экономические аспекты и финансовые возможности обеспечения защиты прав субъектов персональных данных.

7. Технические возможности[2]

До сих пор сохраняет свою актуальность тезис Чарльза Рааба, профессора государственного управления и сравнительной политологии Эдинбургского университета, признанного эксперта в сфере информационной приватности: «консенсус в отношении баланса ценностей пока не достигнут даже на теоретическом уровне»[3]. Поэтому аргументированное решение задачи защиты персональных данных – это всегда непростой процесс анализа последствий с учетом интересов различных сторон в конкретной ситуации. При этом никакое решение не может быть окончательным. А широкое общественное обсуждение должно стать гарантией того, что новые вызовы и возможности ответов на них

---

[1] Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf

Bygrave, L. (2010) Privacy and data protection in an international perspective. Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf; Raab, Ch. (1999) Governing Privacy: Systems, Participants and Policy Instruments// Proceedings of Ethicomp99: Fifth International Conference, Rome, 1999.

[2] Bygrave, L. (2010) Privacy and data protection in an international perspective. Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf; Raab, Ch. (1999) Governing Privacy: Systems, Participants and Policy Instruments// Proceedings of Ethicomp99: Fifth International Conference, Rome, 1999.

[3] Raab, Ch. (1999) Governing Privacy: Systems, Participants and Policy Instruments// Proceedings of Ethicomp99: Fifth International Conference, Rome, 1999

в достаточной степени учитываются при разработке стратегий.

Такой диалог является крайне важным и в современном беларусском контексте.

Все больше данных собирается государственными органами, все активнее развивается интернет-бизнес. Информация о предпочтениях, поведении и пр. становится капиталом. При этом законодательство не гарантирует в достаточной степени защиту прав субъектов персональных данных, а граждане плохо осведомлены о том, как обращаются с их персональными данными.

Все это негативно влияет на цифровое доверие, один из основных элементов успешного развития информационного общества в Беларуси. В «Национальной программе ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы» отмечается, что сведение к минимуму злоупотреблений персональной и иной конфиденциальной информацией – необходимое условие расширения использования электронного документооборота, ведения электронной торговли, предоставления электронных услуг, широкомасштабного внедрения систем электронных платежей[1].

2015 год- это год подведения итогов выполнения национальных программ и стратегии развития информационного общества. 2015год – это год принятия решений о приоритетах, когда в связи с внедрением геолокационных и облачных сервисов, технологий распознавания лиц, ростом числа пользователей социальных сетей:

- появляются новые персональные данные (cookie, IP, UID, трэкирование, распознавание лиц и т.п.);
- возникает необходимость новых ограничений,
  - на объединение данных (profiling),
  - на трансграничную передачу и хранение данных;
- первостепенное значение приобретает принцип минимизации данных;
- изменяется субъектный состав и, соответственно, принципы разделения ответственности;
- принципиальный характер приобретает проблема анонимности на будущее.

В этой ситуации актуализируется необходимость обсуждения проблематики защиты персональных данных, поиска аргументированного ответа на вопросы о том, что

[1] Национальная программа ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы. Постановление Совета Министров Республики Беларусь, 28 марта 2011 г. № 384. Доступно через: http://www.mpt.gov.by/File/Natpr/natpr_19_03_2014.pdf

ВВЕДЕНИЕ

Цель данного документа заключается в том, чтобы инициировать дискуссии по двум принципиальным вопросам:

- *права субъектов персональных данных,*
- *ответственность организаций (государственных и коммерческих), использующих эти данные.*

должно защищаться, как должно защищаться (инструменты политики) и кем должно защищаться (акторы).

Цель данного документа заключается в инициировании дискуссии по двум принципиальным вопросам, которые в значительной степени определяют позиции в отношении политики защиты персональных данных:

- права субъектов персональных данных,
- ответственность организаций (государственных и коммерческих), использующих эти данные.

Из всего комплекса взаимосвязанных проблем акцент сделан, прежде всего, на балансе приватности и безопасности (раздел «Что угрожает цифровому доверию?», «Защита персональных данных: между приватностью и безопасностью»). В разделе «В чём суть проблемы?» инструменты защиты прав субъектов персональных данных и акторы, которые связывают свои решения с регулированием в этой сфере, охарактеризованы на основании анализа и международного опыта. В разделе «Защита персональных данных в Беларуси» проблема структурирована по трем параметрам: содержание понятий, инструменты, акторы. В выводах предлагаются обобщенные рекомендации относительно возможных направлений деятельности и тематики общественных дискуссий.

Анализ политики в отношении защиты персональных данных основан на теоретических подходах, предложенных А. Уэстином, Ч. Раабом, К. Беннетом, Л. Байгрэйв и К. Гринфилдом[1]. В рамках этих подходов

[1] Westin, A. (2003) Social and Political Dimensions of Privacy. Доступно через: http://www.asc.upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf; Bennett, C. (2001) What Government Should Know about Privacy: A Foundation Paper. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf; Bennett, C. (2008) The Privacy Advocates: Resisting the Spread of Surveillance. Cambridge, MA: MIT Press; Bennett, C. Grant, R. (1999) Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press; Bennett, C. and Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge, MA: The MIT Press; Bygrave,

эффективный режим политики в отношении персональных данных определяется как использование комплекса разнообразных инструментов регулирования и вовлечением различных кластеров акторов в процессы структурирования проблемы защиты персональных данных и принятия решений в этой сфере.

За пределами анализа остаются дискуссии, связанные с пересмотром директивы о защите персональных данных Европейского Союза, руководящих принципов ОЭСР, инициативы Всемирного банка и международных правозащитных организаций. Включение в эти дискуссии невозможно без позиционирования в отношении базовых принципов в рамках обозначенной проблемы, которые рассматриваются в данном документе.

L. (2002) Data Protection Law: Approaching its Rationale, Logic and Limits. The Hague: Kluwer Law International; Greenleaf, G. (2011) Global Data Privacy in a Networked World. Доступно через: http://ssrn.com/abstract=1954296

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕЖДУ ПРИВАТНОСТЬЮ И БЕЗОПАСНОСТЬЮ

Защита персональных данных: между приватностью и безопасностью

ПРИВАТНОСТЬ И ПРАВО НА ПРИВАТНОСТЬ

Частная (личная) жизнь – это емкая категория, которой невозможно дать исчерпывающее определение. Каждый человек волен развивать это понятие и наполнять его определенным смыслом. Было бы непозволительно ограничить понятие [личной жизни] «внутренним кругом» и целиком исключить внешний мир, не входящий в этот круг. Таким образом, понятие личной жизни с необходимостью включает право на развитие взаимоотношений с другими лицами и внешним миром[1].

Хотя общепринятой трактовки понятия «частная жизнь» не существует, большинство теоретиков сходятся в том, что термином «частная жизнь» обозначаются:

- сферы жизни человека, которые он не желает делать достоянием других (физических и юридических лиц, органов и должностных лиц государственной власти);
- «личное усмотрение» – свобода от внешнего управляющего воздействия и контроля государства, общественных организаций, граждан в рамках этих сфер и возможность контролировать их[2].

Общим эквивалентом понятия «неприкосновенность частной жизни» и термина «privacy», используемого в международных документах, является заимствованное из латинского языка слово «приватность» в значениях свобода, интимность, секретность, одиночество, собственность, личность, межличностные отношения.

Общим эквивалентом понятия «неприкосновенность частной жизни» и термина «privacy», используемого в международных документах, является заимствованное из латинского языка слово «приватность» в значениях свобода, интимность, секретность, одиночество, собственность, личность, межличностные отношения[3].

---

[1] Красотенко, О. Понятие «частная жизнь» в решениях Европейского Суда по правам человека. Минск, 2011. Доступно через: http://elib.bsu.by/handle/123456789/29040

[2] Шахов Н.И. (2008) Отношения по охране частной жизни и информации о частной жизни как объект теоретико-правового исследования. Ростов-на Дону. С. 7

[3] Прохвачева, О. (2000) Лингвокультурный концепт "приватность": На материале американского варианта английского языка. Доступно через: http://www.dissercat.com/content/lingvokulturnyi-kontsept-privatnost-na-materiale-amerikanskogo-varianta-angliiskogo-yazyka#ixzz3AMsvTYM; Мельников, М. В. (2012) О

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕЖДУ ПРИВАТНОСТЬЮ И БЕЗОПАСНОСТЬЮ

Обеспечение права на неприкосновенность частной жизни (права на приватность) означает установление и соблюдение пределов допустимого вмешательства в частную жизнь.

Пределы допустимого вмешательства определяются:

- физически – границами между публичным и частным, определяющими пространство, в которое организации, правительства или другие люди не могут вторгаться (здесь важно не забывать и о биометрических данных как «эквиваленте тела» индивида);
- в сфере поведения – формы деятельности и образ действий, которые индивид имеет право защищать (скрывать) от внимания посторонних – интимность;
- в сфере принятия индивидуальных решений – человек должен быть защищен от вторжения в эту сферу, то есть от давления на него при осуществлении индивидуального выбора – свобода;
- возможностью человека контролировать информацию о себе – решать, когда, как и в каком объеме, информация о личности становится известной или сообщается другим[1].

Эти границы «частного» не абсолютны, а в значительной степени зависят от контекста, в рамках которого определяются нормы защиты частной жизни и требования того, что может и должно быть раскрыто для общества[2]. Границы информационной приватности также подвижны и основаны на желании или нежелании индивида сообщать ту или иную информацию о себе[3].

Проблема обеспечения права на приватность имеет, как минимум, три измерения: социально-этическое, политическое, инструментальное. С социально-этической точки зрения право на приватность предполагает защиту достоинства, индивидуальности, «личного пространства» человека[4]. Фундаментальная проблема здесь – недопущение потери индивидом достоинства, автономии, уважения вследствие утраты контроля над обстоятельствами, при которых возможно вторжение в реальное (физическое) и

семантике понятия "приватное" // XIII международная научная конференция преподавателей, аспирантов и студентов НСИ. С.181-189

[1] Westin, A. (2003) Social and Political Dimensions of Privacy. Доступно через: http://www.asc.upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf

[2] Schoeman, F. (1992) Privacy and Social Freedom. Cambridge, U.K.: Cambridge University Press.

[3] Westin, A. (2003) Social and Political Dimensions of Privacy. Доступно через: http://www.asc.upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf

[4] Bennett, C. (2008) The Privacy Advocates: Resisting the Spread of Surveillance. Massachusetts Institute of Technology. P.4

виртуальное (цифровое, телекоммуникационное) личное пространство, интимное поведение, принятие решений[1]. Политическое измерение неприкосновенности частной жизни связано с тем, что автономия индивида – это одно из условий и существенных характеристик демократии, которое предполагает недопущение тотального полицейского надзора, свободу собраний, свободу исследований от контроля государства и пр.[2] Инструментальное измерение права на приватность предполагает, что «правильные люди используют правильную информацию о личности в правильных целях», а индивид (субъект персональных данных) имеет возможность контролировать сбор, обработку, использование и раскрытие информации о себе[3].

ИНФОРМАЦИОННАЯ ПРИВАТНОСТЬ

Информационная составляющая частной жизни включает:

> Право на информационную приватность – право индивида контролировать все информационные процессы, связанные со сбором и использованием персональных данных, независимо от того, какая персональная информация собиралась о нем частными и государственными организациями.

- любого рода фактические данные о событиях, связанных с телом человека: факты о болезни лица, составляющие медицинскую тайну; сведения о терапевтическом или хирургическом лечении; фактические данные о смерти и о судьбе человеческих останков;
- фактические сведения, затрагивающие семейную жизнь: персональные данные, кроме общедоступных данных гражданского состояния; о фактах рождения; о фактах заключенных браков; о фактах смертей; о секрете материнства и о секрете усыновления;
- сведения о фактах сексуальной жизни и о чувствах лица; о фактах существования любовных отношений вне семьи или о факте их разрыва;
- сведения о внутренних убеждениях индивида: политические и философские взгляды[4]

---

[1] Rule, J.et al. (1980) The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York: Elsevier

[2] Westin, A. 1(1967) Privacy and freedom. ,P.25

[3] Bennett/ C/ (2008) Bennett, C. (2008) The Privacy Advocates: Resisting the Spread of Surveillance. P..5

[4] Bernard A. La protection de l'intimité par la droit privé: eloge du ragot ou comment vices exposes engendrent vertu. Les For Interieur, p.153-179. Доступно через http://www.u-

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕЖДУ ПРИВАТНОСТЬЮ И БЕЗОПАСНОСТЬЮ

Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении *таких данных*

"персональные данные" означают любую информацию, связанную с идентифицированным или идентифицируемым физическим лицом ("субъектом данных"); идентифицируемым лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности,

посредством ссылки на идентификационный номер или на один, или несколько факторов, специфичных для его физической, психологической,

ментальной, экономической, культурной или социальной идентичности;

Право на информационную приватность – право индивида контролировать все информационные процессы, связанные со сбором и использованием персональных данных, независимо от того, какая персональная информация собиралась о нем частными и государственными организациями, так и способы ее обработки и распространения[1].

Определения приватности индивида в терминах права на контроль использования информации о себе – один из основных тенденций в политических и юридических дискуссиях о защите персональных данных[2].

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Понятие «персональные данные» в широком смысле включает факты, сообщения или мнения, связанные с определенным индивидом и относительно которых разумно было бы ожидать, что он считает их интимными или конфиденциальными, и, следовательно, не желает предавать их огласке или, по крайней мере, желает ограничить их обращение. С этой точки зрения «защита персональных данных» может считаться своего рода аналогом термина «информационная приватность» и в этом смысле предполагает право индивидов решать, когда, какая и в каком объеме информация о них может сообщаться другим.

picardie.fr/labo/curapp/revues/root/35/alain_bernard.pdf_4a081e8ad4544/alain_bernard.pdf (Цит по Ариков, Г. (2014) Аспекты неприкосновенности частной жизни в уголовном законодательстве Республики Молдова. Кишинев, Молдавский государственный университет

[1] В контексте права на информационную приватность анонимность определяется как функциональная неидентифицируемость персонального сообщения. Конфиденциальность означает защиту персональной информации, обычно в форме ограждения этой информации от несанкционированного раскрытия третьим лицам.

[2] Bygrave, L. (2010) Privacy and data protection in an international perspective. Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕЖДУ ПРИВАТНОСТЬЮ И БЕЗОПАСНОСТЬЮ

Понятия «сведения, составляющие тайну индивида» и «персональные данные» не являются идентичными. Персональные данные (такие как, к примеру, фамилия, имя, отчество, образование, профессия) личной тайны не содержат, но позволяют идентифицировать того или иного человека. Отсюда определение персональных данных в узком смысле – любые данные или совокупность данных, которые позволяют идентифицировать индивида.

Кроме того, выделяют (в частности, в государствах-членах ЕС) особую категорию персональных данных – чувствительную информацию (sensitive personal data), обращение с которой требует особой правовой регламентации и более строгих мер защиты[1].

По критерию чувствительности/уязвимости персональные данные подразделяются на три категории

- «обычные» персональные данные - их сбор, обработка, использование и передача возможны без специального разрешения в режиме, предписанном национальными законами;
- «чувствительные» персональные данные - их сбор, обработка, использование и передача требуют особых мер защиты и безопасности, специально установленных законом;
- «особо чувствительные» персональные данные - их сбор, обработка, использование и передача либо вообще запрещены законом, либо разрешены только в исключительных случаях с использованием специальных мер защиты и безопасности.

Набор «особо чувствительных» персональных данных, подлежащих тщательной защите, может варьироваться в различных странах, но, как правило, к этой категории относятся данные о расовом и этническом происхождении, религиозных верованиях, политических убеждениях, членстве в профессиональных ассоциациях, политических и общественных организациях, состоянии здоровья, особенностях сексуального поведения, криминальном прошлом (данные о вынесенных и исполненных обвинительных судебных приговорах по уголовным делам).

---

[1] Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных». Ст. 8 Доступно через: http://books.ifmo.ru/file/pdf/1570.pdf

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕЖДУ ПРИВАТНОСТЬЮ И БЕЗОПАСНОСТЬЮ

Персональные данные – любые данные или совокупность данных, которые позволяют идентифицировать индивида[1].

В США в этом контексте чаще используется термин privacy. В Европе вследствие преобладания инструментального подхода, как правило, маркируют проблему как «защита персональных данных» (data protection). Вместе с тем эксперты отмечают тенденцию возвращения в политический и регуляторный дискурс понятия приватности через термин «приватность данных» (data privacy)[2]. «Приватность данных» определяется через такие категории как невмешательство[3], ограничение доступа[4], контроль информации[5], «чувствительные данные»[6].

Понятие «защита персональных данных» не сводится к требованиям обеспечения качества и безопасности обработки данных, поскольку включает и защиту права субъекта персональных данных контролировать данные о себе.

Понятие «защита персональных данных» не сводится к требованиям обеспечения качества и безопасности обработки данных, поскольку включает и защиту права субъекта персональных данных контролировать данные о себе.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Право на неприкосновенность частной жизни (и, следовательно, право на защиту персональных данных) предполагает, прежде всего, свободу от внешнего вмешательства и возможность контролировать сферу частной жизни.

Информационная безопасность– это обеспечение надежности, целостности и доступности информации и информационных систем посредством защиты их от неавторизованного доступа, разрушения, модификации; защищенность информации и

---

[1] Подробное толкование термина см. в Article 29 data protection working party (2007) Opinion 4/ 2007 on the concept of personal data

[2] Bygrave, L (2010) Privacy and data protection in an international perspective. Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf

[3] Warren, S.D. and Brandeis, L.D., (1890) The Right to Privacy. Доступно через: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[4] Gavison, R., (1980) Privacy and the Limits of Law, Yale Law Journal 1980, vol. 89, p. 421, 428–436 "

[5] Westin, A. (1967) Privacy and Freedom. Доступно через: http://www.jstor.org/

[6] Bygrave, L (2010) Privacy and data protection in an international perspective. Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf.

поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры и т.п. Кибербезопасность – это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии…»[1]

> Информационная безопасность» и кибербезопасность чаще всего трактуются как совокупность мер, предпринимаемых внешними по отношению к индивиду (субъекту персональных данных) структурами (как правительственными, так и коммерческими), которые могут приводить к нарушениям неприкосновенности частной

Термин «информационная безопасность» используется, главным образом, специалистами в сфере ИТ и в отношении организаций; термин «кибербезопасность» чаще используется в политических дискуссиях, когда информационная безопасность рассматривается в рамках национальной безопасности[2] «Информационная безопасность» и «кибербезопасность» в большинстве случаев рассматриваются как синонимы и чаще всего трактуются как совокупность мер, предпринимаемых внешними структурами (как правительственными, так и коммерческими), которые могут приводить к нарушениям неприкосновенности частной жизни[3])

Киберзащита (Cybersecurity)- защищенность информации от угроз конфиденциальности, целостности, доступности в киберпространстве. Кибербезопасность (Cybersafety) - состояние защищенности от физических, социальных, духовных, политических, эмоциональных, профессиональных, образовательных и других типов или последствий аварии, повреждения, ошибки, несчастного случая, нанесения вреда или любого другого события в киберпространстве, которое может рассматриваться как нежелательное[4].

---

[1] Рекомендация МСЭ-Т X.1205, Обзор кибербезопасности. Доступно через: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru)

[2] APC (2013) A cyber security agenda for civil society: what is at stake? Доступно через: http://www.apc.org/en/pubs/cyber-security-agenda-civil-society-what-stake

[3] ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» Доступно через: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[4] Там же

В этом контексте право на информационную приватность может ограничиваться и нарушаться во имя обеспечения безопасности индивида и/или общества[1].

В качестве примера можно привести усиление государственных мер по мониторингу (surveilliance) интернета и других коммуникаций, усиление государственного контроля деятельности операторов связи, расширение возможностей доступа к данным пользователей телекоммуникационных услуг:

- установка специализированных устройств по перехвату интернет-трафика («черные ящики»);
- законодательное закрепление обязанности интернет-провайдеров по хранению интернет-трафика в течение длительного времени;
- отказ от части государственных гарантий по обеспечению приватности и защиты персональных данных;
- упрощение процедурного порядка доступа представителей силовых структур к персональным данным пользователей.

Многие эксперты обращают внимание на то, что результативность таких мер в борьбе с терроризмом и организованной преступностью не соответствует затратам на их внедрение и не оправдывает нарушения права на информационную приватность (в том числа права субъекта контролировать, кто, когда и зачем использует информацию о нем).

Таким образом, защита персональных данных не сводится к обеспечению мер технической безопасности сбора, хранения и обработки данных (качество использования). Более того, принимаемые меры безопасности могут стать причиной нарушения неприкосновенности цифровой сферы частной жизни. Критерием допустимости вмешательства в целях обеспечения безопасности может стать право индивида контролировать использование информации о себе. Баланс между приватностью и безопасностью – сложный вопрос, который не может решаться техническими специалистами, юристами или спецслужбами. Международная практика с очевидностью демонстрирует, что в решении этой проблемы должны принимать участие различные акторы. А регулирование защиты персональных данных должно основываться на использовании разнообразных инструментов.

---

[1] Агапеева, К. (2012) Теория секьюритизации Барри Бузана. Доступно через: http://www.geopolitica.ru/article/teoriya-sekyuritizacii-barri-buzana#.VG2uO_msXzc; Buzan,B., Waever, O. Wilde, J. (1998) Security: A New Framework for Analysis. Доступно через:http://books.google.by/books/about/Security.html?id=j4BGr-Elsp8C&redir_esc=

Что угрожает цифровому доверию

ИЗМЕНЯЮЩИЙСЯ ЛАНДШАФТ ПРИВАТНОСТИ

В Республике Беларусь почти 5 миллионов пользователей сети интернет, что составляет 70% населения в возрасте от 15 до 74 лет. Большинство из них (84%) выходят в сеть каждый день. В стране 11 миллионов абонентов сотовой связи и 10 миллионов контрактов на использование услуг доступа в сеть интернет.

График 1. Рост интернет-аудитории в Беларуси в 2014 г.

В сети ищут информацию (90% пользователей), пользуются сетевыми социальными (70%) и видео-сервисами (55%), читают новости (50 %), осуществляют платежи (20%). Представители Белорусской железной дороги 30 декабря 2014 г. вручили памятный

подарок миллионному интернет-пассажиру 2014 года (система продаж билетов через интернет была введена в опытную эксплуатацию в начале 2011 года)[1].

65% беларусских пользователей интернета хоть раз совершали онлайн-покупки. В 2014 г. онлайн-покупки в Беларуси совершил в среднем 1 млн пользователей[2]. По данным Министерства торговли на август 2014 г. в Беларуси было зарегистрировано 9 627 интернет-магазинов[3].

Интернет прочно вошел не только в жизнь граждан, но и в деятельность предприятий и организаций. Почти все субъекты хозяйствования предоставляют налоговые декларации (91%) и ведомственную отчетность (80,6 %) онлайн. 29,7% организаций – таможенные документы. 18,6% субъектов хозяйствования прошли электронную регистрацию[4].

По данным Белстата на 2013 год, наибольший процент организаций с веб-сайтами – среди финансовых учреждений – 95,7%. Больше половины (67%) организаций, предоставляющих коммунальные, социальные и персональные услуги также присутствуют онлайн. 40,9 % организаций получают заказы онлайн и 53,6% – размещают заказы онлайн[5].

В ближайшие 1-1,5 года беларусское правительство планирует существенно расширить сферу возможностей оказания электронных услуг организациям и гражданам посредством интегрирования государственных информационных ресурсов с общегосударственной автоматизированной информационной системой. А к 1 января 2016 года все госорганы, а также юридические лица с долей государства должны будут подключиться к единой системе электронного документооборота. Для того, чтобы услугами электронного правительства смогли воспользоваться все граждане Беларуси, планируется ввести систему электронной идентификации личности. Уже сейчас значительную часть документов в госорганах получают (42, 35%) и отправляют (31,4%) в электронном виде[6].

---

[1] БЖД вручит памятный подарок миллионному интернет-пассажиру 2014 года. Доступно через:http://www.belta.by/ru/all_news/society/BZhD-vruchit-pamjatnyj-podarok-millionnomu-internet-passazhiru-2014-goda_i_690740.html

[2] Data Insight (2014) Какие тренды на белорусском рынке e-commerce в этом году, Доступно через: http://probusiness.by/markets/154-kakie-trendy-na-belorusskom-rynke-e-commerce-v-etom-godu.html

[3] Число интернет-магазинов в Беларуси за 7 месяцев возросло в 1,5 раза. Доступно через: http://www.belta.by/ru/all_news/economics/Chislo-internet-magazinov-v-Belarusi-za-7-mesjatsev-vozroslo-v-15-raza_i_677634.html

[4] Зиновский В. (2014) Информационное общество в Республике Беларусь, 2014. Доступно через: http://belstat.gov.by/bgd/public_compilation?id=520

[5] Там же

[6] Там же

ЧТО УГРОЖАЕТ ЦИФРОВОМУ ДОВЕРИЮ

Государственные органы собирают и хранят огромные массивы сведений о гражданах в базах данных различных министерств и ведомств.

УГРОЗЫ

Использование персональных данных обеспечит огромную отдачу для правительств, организаций и частных лиц. Но распространение информационно-коммуникационных технологий создает как новые возможности, так и новые риски, в том числе в отношении неприкосновенности частной жизни человека.

Мы оставляем онлайн огромные массивы персональной информации. Ежедневно через почтовые серверы проходят миллиарды электронных писем. Facebook хранит более сотни мегабайт персональных фотографий и видео на каждого пользователя. Через платежные системы проходят сотни миллиардов персонально помеченных финансовых платежей. Большинство совершеннолетнего населения в развитых странах постоянно транслирует свои текущие координаты через мобильные сети.

Пользователи вручают крупным компаниям колоссальные объемы данных о своей повседневной жизни, в том числе и конфиденциальной при этом считая, что компании будут осторожно обращаться с их данными, однако гарантия есть не всегда. Когда же на основе этой информации принимаются неполезные для нас решения, о них обычно не сообщается[1].

Ошибки, возникающие в результате объединения данных различных государственных структур – источник серьезных угроз информационной сфере частной жизни. Существует мнение, что более половины наборов сведений о гражданах, которые собирают правительства, содержат ошибки. Некоторые из этих ошибок, такие как неправильный адрес, несущественны, их легко заметить и исправить. В других случаях может совместиться кредитная информация о двух совершенно разных людях с похожими именами и т.п. При таких обстоятельствах бывает сложно понять основания тех или иных решений, принимаемых соответствующими учреждениями.

Массовая систематическая слежка за гражданами – одна из серьезнейших угроз неприкосновенности частной жизни онлайн. Суть функционирования системы массового систематического слежения сводится к процедуре поиска и выборки персональных данных конкретного субъекта из различных файлов (которые могут храниться в компьютерных банках данных, дислоцированных в разных концах страны) и слияния этих персональных данных в единый файл, содержащий исчерпывающие сведения о данном субъекте данных (data matching – совмещение,

[1] Паризер, Э. (2012) за стеной фильтров. Что интернет скрывает от нас. Москва, Альпина

стыковка, согласование данных). Создание системы «Большого брата» на базе применения процедур типа data matching предполагает наличие единого поискового признака – универсального идентификационного кода.

С развитием систем анализа больших массивов данных (Big Data) угроза усиливается, поскольку объединяться может, не только информация, содержащаяся в базах данных, но и видео, аудиоинформация, наши следы в интернете и пр. Такие системы позволяют установить уникальный профиль человека даже без слежки, а просто путем анализа его перемещений по координатам GSM-телефона и изображению с общедоступных камер наружного наблюдения, а также с помощью анализа интернет-трафика. Сохранить анонимность при генерации столь огромного массива информации становится практически невозможно.

По данным глобальных исследований, большинство лиц, ответственных за защиту персональных данных в компаниях, не имеют достаточно времени для выполнения своих обязанностей, а отчеты руководителям предоставляются нерегулярно. Исследование выявило, что 60% сотрудников компаний чаще всего допускают нарушения именно при обработке персональных данных, и наиболее часто жертвой подобных нарушений является клиент; 50% наиболее распространенных причин, которые приводят к нарушению принципов защиты персональных данных в пределах компании, является небрежность, а в 51% случаев такие нарушения не регистрируются и не наказываются соответствующим образом[1].

Превращение персональной информации в товар – еще одна угроза информационному самоопределению личности. «Идентифицирующая личность информация: имя, профессия, хобби и другие мелочи, делающие человека уникальным, превращается в объект владения, – пишет Э. Паризер. – Но владеют этим объектом не конкретные индивидуумы, контролирующие информацию о себе, а крупный бизнес, постоянно использующий его для получения прибыли и захвата рынка. Как можно ощущать собственную ценность, не владея в полной мере даже собственным именем?»[2].

Существуют специализированные компании, которые собирают общедоступные данные и привязывают их к профилям конкретных людей, с указанием имени, адреса и

[1] 2B Advice (2012) Data Protection Practice 2012. Доступно через: https://www.2b-advice.com/GmbH-en/Study-Data-Protection-Practice-2012

[2] Паризер, Э. (2012) за стеной фильтров. Что интернет скрывает от нас. Москва, Альпина

Основные типы угроз приватности в цифровом мире:

недобросовестная политика обращения с персональными данными со стороны держателей данных (прежде всего, представителей бизнеса, а также со стороны государственных органов), которым были доверены персональные данные со стороны граждан (в том числе и утечка персональных данных);

сбор, систематизация и распространение персональных данных из различных источников, позволяющих составить многосторонний «профиль» соответствующего субъекта данных: от религиозных убеждений и особенностей характера до покупательских предпочтений и сведений об имуществе;

киберпреступность (сетевое мошенничество, вредоносные программы и программы-шпионы, кражи, совершенные посредством использования информационно-коммуникационных технологий).

т.д. Например, американская компания Acxiom уже накопила базу данных по 1500 классификаторам на 500 миллионов пользователей со всего мира. Компания заявляет, что по составленным профилям может прогнозировать реакцию потребителей на различные раздражители (товары, бренды и проч.)[1]. Такие компании способны даже автоматически предсказывать местонахождение пользователей, анализируя архивные GPS-метки. По последним экспериментальным данным, точность составляет 80% в течение 80 недель[2].

Данные, на основании которых можно идентифицировать индивида, собираются не только правительствами и коммерческими компаниями. Пользователи различных ресурсов и сервисов глобальной сети интернет – это сотни тысяч «маленьких братьев», которые поставляют видео, аудио и текстовую информацию о людях онлайн.

Еще одна опасность – это персонализация потоков сообщений, которая лишает человека возможности контролировать информацию, которую он получает. Код, лежащий в основе персонализации, довольно прост, поясняет Э. Паризер: «Фильтры нового поколения изучают то, что вам, судя по всему, нравится: ваши предшествующие действия или то, что нравится людям, похожим на вас, – и пытаются экстраполировать эти данные. Это механизмы предсказаний, постоянно уточняющие теорию о том, кто же вы на самом деле, что вы сделаете и чего захотите дальше. Вместе они творят уникальную информационную вселенную для

---

[1] Tucker, P. (2013) Has Big Data Made Anonymity Impossible?.Доступно через: http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible

[2] Sadilek, A., Krumm, J.(2012) Far Out: Predicting Long-Term Human Mobility. Доступно через: http://www.cs.rochester.edu/~sadilek/publications/Sadilek-Krumm_Far-Out_AAAI-12.pdf

каждого из нас — я называю этот процесс возведением «стены фильтров» — и фундаментально меняют наш подход к восприятию информации»[1]. Тем самым стирается граница между удобством сервиса и вмешательством – контролем поведения и непосредственным влиянием на личность.

Демократизация деструктивных технологий, информационные войны, создающие угрозу национальной безопасности, побуждают правительства все в большей степени использовать системы массированного систематического наблюдения. События последних лет показали, насколько опасной для сохранения неприкосновенности частной жизни может быть такая деятельность при отсутствии надлежащих инструментов регулирования.

Непосредственную угрозу информационной приватности представляют различные виды компьютерных преступлений. Большинство из них – это «старые» нарушения неприкосновенности частной жизни, совершенные с использованием информационно-коммуникационных технологий. Некоторые же, например, кража личности – это совершенно новые явления, которые требуют разработки новых мер регулирующего воздействия.

Таким образом, типы угроз приватности в цифровом мире можно обозначить следующим образом:

- недобросовестная политика обращения с персональными данными со стороны держателей данных (прежде всего, представителей бизнеса, а также со стороны государственных органов), которым были доверены персональные данные со стороны граждан (в том числе и утечка персональных данных);
- сбор, систематизация и распространение персональных данных из различных источников, позволяющих составить многосторонний «профиль» соответствующего субъекта данных: от религиозных убеждений и особенностей характера до покупательских предпочтений и сведений об имуществе;
- киберпреступность (сетевое мошенничество, вредоносные программы и программы-шпионы, кражи, совершенные посредством использования информационно-коммуникационных технологий).

Иными словами, угрозы информационной приватности порождаются не применением новых цифровых и телекоммуникационных технологий, а ненадлежащими способами

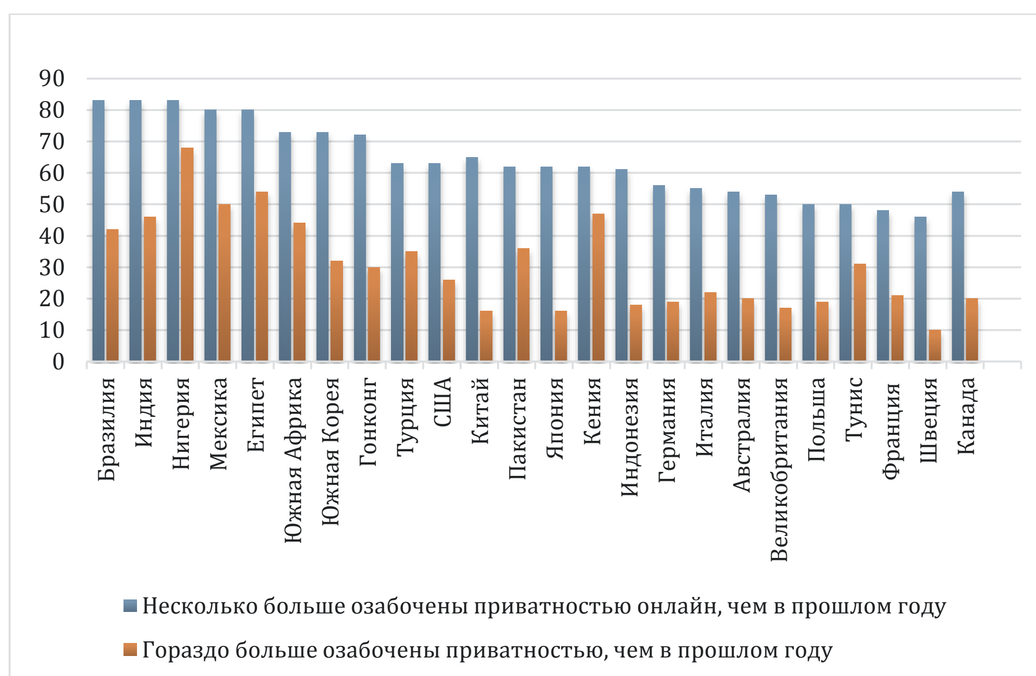
[1] Там же

сбора информации (массовое систематическое слежение, перехват сообщений, опросы, анкеты и пр.) и несоблюдением необходимых мер защиты при обработке информации.

....И КАК МЫ НА НИХ РЕАГИРУЕМ

По данным глобальных исследований, люди все больше ощущают угрозы неприкосновенности частной жизни онлайн.

График 2. Ответы на вопросы о приватности онлайн. Распределение по странам (%) [1]



В Беларуси не проводилось полномасштабных исследований того, как на практике государственные и частные организации обращаются с теми объемами персональных данных, которые оказываются в их распоряжении. Не исследовались и установки пользователей ресурсов и сервисов сети интернет в отношении права на неприкосновенность частной жизни онлайн. Однако есть все основания предположить, что Беларусь в этом отношении не является исключением и многие тенденции, обозначенные в предыдущем разделе, проявляются и в нашей стране.

Результаты опроса 40 активистов общественных организаций, проведённого аналитической группой ЦЕТ совместно с Центром правовой трансформации,

[1] CIGI-IPSOS Global Survey on Internet Security and Trust. Доступно через https://www.cigionline.org/internet-survey

позволяют отметить наличие озабоченности в отношении защиты цифровой приватности.

График 3. Обеспокоенность в отношении защиты персональных данных

При этом практически все предложенные к оценке области использования интернет, по мнению респондентов, несут в себе потенциальные опасности, связанные с возможностью злоупотребления персональной информацией пользователей.

Таблица 1. Основные угрозы цифровой приватности

В каких ситуациях использования сети интернет Вы чувствуете наибольшую угрозу, связанную с возможными злоупотреблениями Вашей персональной информацией? (возможно несколько вариантов ответа)	Абсолютная частота
При использовании почтовых сервисов	24
Когда Вы заходите на сайт, который требуют регистрации	23
При пользовании социальными сетями	22
При покупке товаров или услуг	20
Не чувствую никаких угроз	0

Большинство (64 %) при этом осознает, что угрозы не очевидны, имеют скрытый характер.

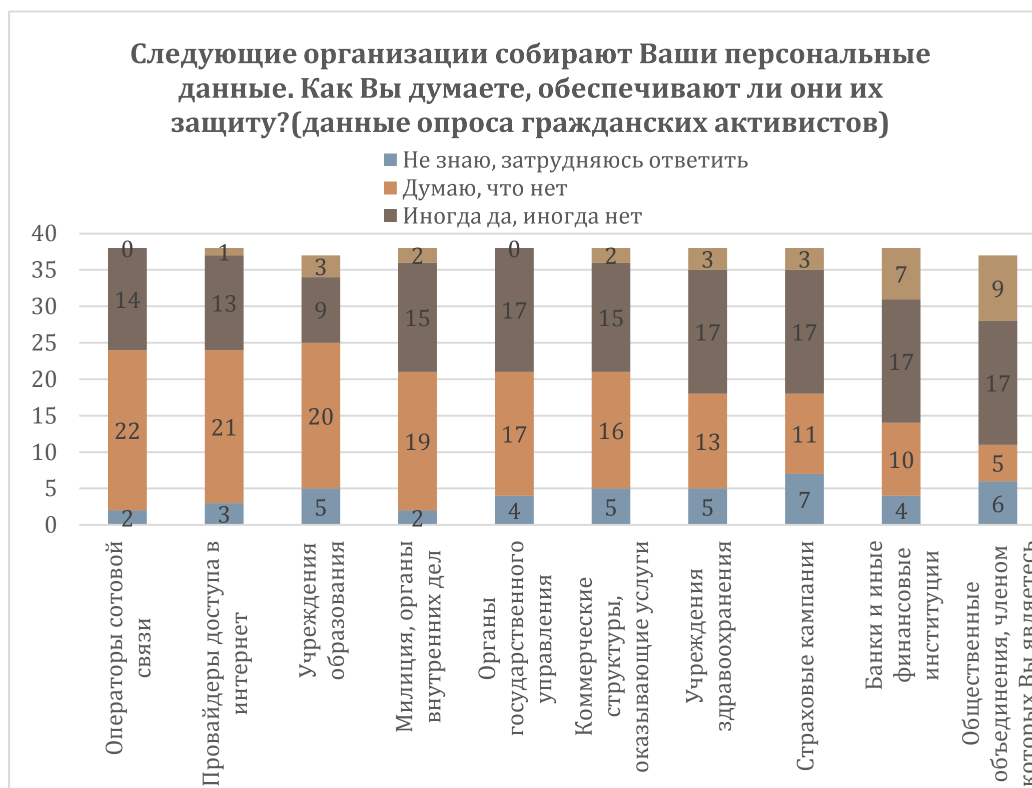
График 4. Нарушения приватности онлайн

Как показывают ответы на последующие вопросы, эти злоупотребления связаны чаще всего с передачей и использованием не по назначению контактных данных (телефон, адрес электронной почты) или отслеживанием информации в социальных сетях.

В ходе работы фокус-групп так же было озвучено несколько кейсов и несколько наиболее распространенных типов злоупотреблений персональными данными с последствиями разной степени тяжести: от огромного количества навязчивой рекламы в социальных сетях, поисковиках или непосредственно в электронной почте, до финансовых потерь (воровство денег с карточек) и попадания в почти уголовную историю.

В то же время, во многих случаях некорректное обращение с персональными данными происходит не по злому умыслу и не в целях личной выгоды (или «государственных интересов»), а просто по незнанию и от безграмотности. В ходе работы фокус-групп были озвучены несколько случаев такого рода: региональная газета публиковала персональные данные всех «новых граждан города» (то есть личные данные новорожденных и матерей), пока одна из матерей не пригрозила журналистам судом; сайт государственной поликлиники, который ввел возможность заказывать талоны на посещение врача онлайн, сделал информацию о том, кто к какому врачу записывается общедоступной и пр.

График 5. Уровень доверия организациям в сфере защиты персональных данных



Никто из респондентов не имеет полной уверенности, что организации (государственные и частные), собирающие, хранящих и обрабатывающих информацию, обеспечивают необходимый уровень защиты персональных данных.

Интересно, что опрошенные гражданские активисты не имеют однозначного и твёрдого мнения по вопросу о публичном раскрытии информации о частной жизни конкретных людей: примерно половина (16 из 35) считают, что в некоторых случаях нарушение тайны частной жизни допустимо, тогда как только немного меньше (13 из 35) считают, что необходим законодательный запрет на публичное раскрытие личной информации.

Что касается способов зашиты персональной информации, то среди гражданских активистов равно распространены следующие:

- осторожность – избегать сомнительных сайтов, не оставлять самим личных данных в открытом доступе, использовать анонимизаторы, управление паролями,
- использование специального ПО: PGP, TrueCrypt,
- изменение законодательства – например, законы, запрещающие компаниям (интернет-провайдерам и др.) предоставлять «на сторону» личные данные граждан,

- смирение – или отказаться от использования интернета и современных технологий, или просто иметь в виду риски и опасности; пользоваться интернетом на свой страх и риск.

Анализ результатов опроса активистов общественных организаций и работы в фокус-группах (журналисты и представители бизнеса) показал:

- обыденные примеры «социального дискомфорта» не связываются с правом на неприкосновенность частной жизни онлайн;
- термин «персональные данные» становится все более узнаваемым, однако интерпретации его неоднозначны и иногда далеки от реального содержания;
- степень защищённости персональных данных, собираемых государственными и коммерческими учреждениями, вызывает серьезные опасения, которые, в силу специфики регулирования этой сферы в Беларуси, трудно подтвердить или опровергнуть;
- отсутствие общих регламентов и правил, регулирующих обращение с персональными данными, их хранение, передачу или распространение, только в незначительной степени компенсируется некодифицированными нормами (здравый смысл, моральные нормы, журналистская этика) или внутрикорпоративными регламентами;
- в качестве мер, которые могли бы способствовать улучшению ситуации и повышению защищенности граждан, респондентами исследования предлагалось введение единого законодательного регулирования процессов сбора, хранения и распространения персональных данных, а также просветительские и образовательные действия, направленные на повышение компетенций граждан в обращении с личной информацией.

Политика в отношении персональных данных имеет многоуровневый и кросс-секторальный характер. В нее вовлечены наднациональные, национальные и субнациональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные.

В чем суть проблемы?

АКТОРЫ

Политика в отношении персональных данных имеет многоуровневый и кросс-секторальный характер. В нее вовлечены наднациональные, национальные и субнациональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные.

Актор публичной политики – это «действующее лицо», которое принимает активное участие в процессе решения социально значимых проблем и характеризуется, по крайней мере:

- свободой маневра по отношению к принуждениям системы;
- способностью взаимодействия с другими;
- способностью к активному поведению;
- наличием стратегии (цель и способы ее достижения);
- признанием со стороны других акторов[1].

Существуют различные подходы к анализу сложной структуры акторов публичной политики[2]. Наиболее подходящим для первоначального введения в проблематику защиты персональных данных представляется структурирование на основании формальной/официальной позиции, предложенной К. Бенентом и Ч. Раабом[3].

[1] В зависимости от того или иного подхода к политическому анализу, исследователи используют и по-разному определяют термины агент действия, субъект политики, актор и пр. Авторы данного пособия руководствуются дефинициями, обоснованными в книге Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J. and Bots, P. (2010) Policy Analysis of Multi-Actor Systems. P. 79-108. Следует также отметить, что в рамках теории организаций чаще используется термин «стейкхолдер», который исторически предшествовал теоретическому оформлению понятия «актор политики».

[2] Подробно эти подходы описаны здесь Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J. and Bots, P. (2010) Policy Analysis of Multi-Actor Systems.

[3] Raab, C., Koops, B-J (2009), 'Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.edu

Исследователи, прежде всего, обращают внимание на то, что транснациональное «движение» персональных данных в глобальной сети обуславливает фундаментальное значение международных принципов и, следовательно, определяющую роль **глобальных и региональных межправительственных организаций и объединений**: ООН, ОЭСР, Совета Европы, Европейского Союза, Организации Азиатско-Тихоокеанского сотрудничества, Всемирного банка, Всемирной торговой организации, Международной торговой палаты и др.

Для того, чтобы установить единообразный режим правового регулирования обработки и передачи персональных данных в рамках союза или сообщества стран, представляющая его международная организация, как правило, последовательно выполняет следующее:

- добивается консенсуса стран-участниц данного сообщества относительно тех принципов защиты данных, которые должны применяться в рамках сообщества,
- легитимизирует эти принципы при помощи подписания странами-участницами соответствующего международного соглашения, предусматривающего обязанность стран-участниц гармонизировать свое национальное законодательство в соответствии с вышеуказанными принципами защиты данных,
- устанавливает для стран-участниц, ратифицировавших вышеупомянутое международное соглашение и гармонизировавших национальное законодательство, режим наибольшего благоприятствования в сфере обмена персональными данными,
- запрещает (или, по крайней мере, строго ограничивает) обмен персональными данными со странами, не являющимися участницами данного международного соглашения о защите данных как напрямую, так и через третьи страны[1].

На национальном уровне важнейшую роль в разработке и реализации политики в отношении приватности, безусловно, играют **законодатели, суды и органы высшей государственной власти.**

Очевидно, что и **исполнительные органы, государственные учреждения и организации,** обеспечивающие процессы сбора, хранения и обработки данных, также существенно влияют на политику в отношении защиты персональных данных. Их роль и влияние определяются функциями в различных контекстах (см. таблицу «Пример: функции и контексты акторов политики в отношении защиты персональных данных»).

[1] Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Только серьёзный анализ таких кластеров интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий.

К числу ведущих институциональных акторов К. Беннет и Ч. Рааб относят также **уполномоченные органы по защите прав субъектов персональных данных** и их международные объединения.

Функции национального органа (или системы органов) по обеспечению качества персональных данных и защите прав субъектов данных (традиционно такие органы называют кратко – «органы защиты персональных данных»):

- регистрационно-разрешительные,
- контрольно-надзорные,
- арбитражные,
- экспертные.

Неправительственные институциональные акторы – крупные интернет-компании (в лице ответственных или департаментов по защите прав субъектов персональных данных) составляют еще одну влиятельную группу акторов. Так, в 1983 г. была создана Международная рабочая группа по защите персональных данных в сфере телекоммуникаций (Берлинская группа), которая опубликовала ряд влиятельных в рамках европейской политики документов[1]. Альянс онлайновой приватности (Online Privacy Alliance: http://www.privacyalliance.org/)– бизнес-ассоциация, содействующая разработке правил и принципов саморегулирования в целях обеспечения защиты персональных данных потребителей. В 2008 г. была создана ассоциация «Глобальная сетевая инициатива (Global network initiative: https://www.globalnetworkinitiative.org/), члены которой в рамках стратегий социальной корпоративной ответственности разрабатывают критерии и меры обеспечения защиты персональных данных в сфере ИКТ-индустрии. Рабочая группа по приватности и защите персональных данных Международной торговой палаты –

---

[1] International Working Group on Data Protection in Telecommunications. Доступно через: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt

единственная бизнес-ассоциация, имеющая статус наблюдателя в комитете по защите персональных данных Совета Европы[1].

Группы активистов защиты прав субъектов персональных данных формируются и функционируют на национальном и наднациональном уровнях. Такие организации, как Electronic Privacy Information Center, Privacy International оказывают существенное влияние на формирование принципов и механизмов регулирования. Особый интерес, с точки зрения экспертов, представляет организация «Европейские цифровые права» (European Dgital Rights/EDRI), созданная в 2002 г. и объединяющая 29 групп из 18 европейских стран[2]. В частности, EDRI подготовила популярную брошюру «Защита персональных данных. Введение»[3].

Серьезным вкладом в обеспечение прав субъектов персональных данных стали «Международные принципы применения прав человека в отношении мониторинга средств связи», которые были разработаны общественными организациями Access, Article 19, Association for Progressive Communications, Bits of Freedom, Electronic Frontier Foundation, European Digital Rights, Privacy International и др[4].

Правозащитники, усматривающие в отдельных законодательных инициативах и действиях правительства угрозу правам человека (главным образом, праву на неприкосновенность частной жизни). Этих активистов объединяет общая обеспокоенность существующими тенденциями законодательного регулирования обращения персональных данных (при этом указывается, во-первых, на меньшую проработанность соответствующих нормативных инициатив по сравнению с европейским уровнем, а также их несоответствие интересам российских граждан [2]), отсутствием выраженной готовности органов государственной власти к диалогу, низким уровнем правосознания российских граждан.

Среди влиятельных акторов **– организации, устанавливающие технические стандарты**:

- Международная организация стандартизации,
- Форум информационной безопасности (https://www.securityforum.org/)[5],

---

[1]International chamber of commerce (2008) Privacy and Personal Data. Доступно через: http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/digitaleconomy/privacy-and-personal-data-protection

[2] Raab, C, Koops, B-J (2009), 'Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf

[3]EDRI (2012) Защита персональных данных. Введение». Доступно через: http://www.lawtrend.org/information-access/zashhita-dannyh

[4] International Principles on the Application of Human Rights to Communications Surveillance. Доступно через: https://en.necessaryandproportionate.org/

[5] The Standard of Good Practice for Information Security, Information Security Forum (2003). Доступно через: http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf

- Европейский комитет стандартизации (http://www.cenelec.eu/),
- Британский институт стандартов http://www.bsigroup.com/en-GB/[1].

Обладающие «более, чем средней» степенью правосознания граждане, сетевые активисты, обеспокоенные угрозой нарушения их права на приватность и неприкосновенность персональных данных, также не являются консолидированной стороной. Они обладают различным уровнем компетенции в данном вопросе и участвуют в развитии законодательного процесса с большей или меньшей степенью непостоянства. Тем не менее, представители этой группы играют, возможно, наиболее значительную роль в просвещении интернет-общественности в отношении проблемы обеспечения приватности путем распространения соответствующих публикаций на персональных сайтах и в специализированных изданиях

Таблица 2. Основные акторы политики в отношении персональных данных[2]

Актор	Функция
Разработчик конституции	Обеспечивает право на приватность (и защиту персональных данных)
Законодатель	Разрабатывает закон о защите персональных данных, а также другие законодательные акты с учетом права субъекта данных на защиту персональных данных
Уполномоченный орган по защите прав субъектов персональных данных	Контролирует исполнение законов, способствует распространению лучших практик, инициирует привлечение внимания общественности к вопросам защиты персональных данных
Контролеры данных	Принимают решения относительно целей обработки и типа данных, которые должны быть обработаны
Сотрудники государственных органов	Исполнение законов, обучение персонала правилам и принципом защиты прав субъектов персональных данных
Частные компании	Исполнение законов, обучение персонала правилам и принципом защиты прав субъектов персональных данных, разработка

[1] BS 7799-3:2006.Standard on Information Security Management Systems–Guidelines for Information Security Risk Management. Доступно через: http://www.iso.staratel.com/ISO17799/Doc/BS7799.3.1999/BS%207799-3-2006.pdf

[2] Raab, C., Koops, B-J (2009) 'Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf

	и исполнение корпоративных кодексов, лоббирование тех или иных решений
Гражданские ассоциации, группы активистов	Борются за защиту прав субъектов персональных данных, предлагают решения, рекомендуют, привлекают внимание общественности
Академическое сообщество (правоведы, социологи, философы)	Исследование и проблем защиты прав субъектов персональных данных, выявление долговременных тенденций, прогнозы, рекомендации
Журналисты	Освещают события и проблемы, объясняют политику и тенденции развития, обнародуют факты нарушения прав субъектов данных
Субъекты данных (граждане, потребители)	Защищают свое право на приватность информационной сферы, жалуются
Разработчики технических стандартов и технологий	Разрабатывают стандарты и решения, обеспечивающие защиту персональных данных, обучают ИТ- специалистов

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Эксперты утверждают, что только серьёзный анализ таких кластеров интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий

ИНСТРУМЕНТЫ

Международные принципы

Формальный нормативный базис законодательства о защите персональных данных составляют фундаментальные права человека, зафиксированные в международных и региональных документах:

- Всеобщей декларации прав человека (ООН, 1948) ст. 19, 29;
- Международном пакте о гражданских и политических правах (ООН, 1966) ст. 15;
- Международном пакте об экономических, социальных и культурных правах (ООН, 1976);

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Набор инструментов политики в отношении защиты персональных данных включает не только меры законодательного регулирования, но и транснациональные принципы, руководства и соглашения, практики саморегулирования, стандартизации, технологические решения и просветительские мероприятия. Закон должен дополняться кодексами поведения и технологическими мерами, опираться на соответствующую организационную культуру и поддержку общественности

- Международной конвенции о ликвидации всех форм расовой дискриминации (ст.5);
- Международной конвенции о ликвидации всех форм дискриминации женщин (1965 г.);
- Конвенции о защите прав человека и основных свобод (Совет Европы, 1950) ст. 10, 15, 16, 17;
- Американской декларации прав и свобод человека (1948) ст. 6;
- Американской конвенции о правах человека (Пакт Сан-Хосе, 1969) ст. 13;
- Африканской Хартии прав человека и народов (Организация африканского единства, 1981) ст. 9, 27, 29;
- Хартии социальных прав и гарантий граждан независимых государств (СНГ, 1994);
- Хартии Европейского союза об основных правах человека (ЕС, 2000);
- Арабской хартии прав человека (Лига арабских государств, 2004);
- Конвенции Содружества Независимых Государств о правах и основных свободах человека (СНГ, 2011);
- Азиатской хартии по правам человека (АСЕАН, 2012);
- Бишкекской декларации ОБСЕ.

Международное соглашение на глобальном уровне о принципах защиты персональных данных до сих пор отсутствует, хотя эксперты все более настойчиво говорят о необходимости разработки такого документа. В настоящее время эту лакуну заполняют:

- Резолюция Генеральной ассамблеи ООН «Право на приватность в цифровую эпоху» (2014);
- Резолюция Генеральной ассамблеи ООН «Руководящие принципы, касающиеся компьютеризированных картотек, содержащих данные личного характера» (1990);

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

- Конвенция № 108 Совета Европы о защите индивидуумов (частных лиц) по отношению к автоматизированной обработке персональных данных (1981) и Дополнительный протокол, который вышел за рамки регионального документа и открыт для подписания неевропейскими странами;
- «Рекомендации в отношении Руководящих принципов по защите неприкосновенности частной жизни и трансграничных потоков персональных данных» Организации экономического сотрудничества и развития.

Особое место в этом контексте занимает Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных»[1], которая, по мнению экспертов, определяет основные тенденции законодательного регулирования защиты персональных данных, поскольку:

- принцип адекватности национальных законов требованиям Директивы определяет возможности обмена данными со странами Европейского Союза;
- требования Директивы N 95/46/ЕС дублируются в Дополнительном протоколе Конвенция № 108 Совета Европы.

В рамках СНГ к настоящему моменту существует четыре документа:

Модельный закон СНГ, принятый Межпарламентской ассамблеей в 1999 г.

Решение Координационного Совета государств-участников СНГ по информатизации при РСС от 1 июля 2003 г. N 3/1. «Стратегия сотрудничества стран СНГ в сфере информатизации»

Решение Совета глав правительств Содружества Независимых Государств «О внесении дополнений в Стратегию сотрудничества государств - участников СНГ в сфере информатизации и в План действий по реализации Стратегии сотрудничества государств - участников СНГ в сфере информатизации на период до 2010 года»

Соглашение о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии, и использовании в государствах – участниках СНГ (2009)

[1] Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г.о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года) http://pd.rkn.gov.ru/docs/Direktiva_Evropejskogo_Parlamenta_i_Soveta_Evropejskogo_Sojuz_95_46_ES.rtf

Таблица 3. Принципы защиты данных в международных документах[1].

Принципы защиты данных	Конвенция Совета Европы	Руководящие принципы ОЭСР	Директива ЕС о защите данных
Честные и законные средства сбора данных	✓	✓	✓
Указанные и законные цели сбора данных	✓	✓	✓
Соответствие данных цели их сбора	✓	✓	✓
Точность данных	✓	✓	✓
Хранение данных только до момента достижения цели их сбора	✓	-	✓
Особый режим обращения с «уязвимыми данными»	✓	-	✓
Безопасность обработки и хранения данных	✓	✓	✓
Информирование субъекта данных об осуществлении обработки его данных	✓	✓	✓
Доступ субъекта данных к своим личным данным и возможность их изменения	✓	✓	✓
Подотчетность при обработке данных	✓	✓	✓

Международные принципы защиты персональных данных – не статичный инструмент. С появлением новых технологий, осознанием новых вызовов производится их периодический пересмотр.

В 2013 г. были опубликована новая редакция Руководящих принципов ОЭСР[2].

В новой редакции сохранены все основные принципы:

- законный и ограниченный сбор персональных данных, получаемых с ведома и согласия физического лица,

[1] Tan J (2008) A comparative study of the APEC privacy framework: A new voice in the data protection dialogue?. In Asian Journal of Comparative Law, 3(1). http://www.degruyter.com/dg/viewarticle/j$002fasjcl.2008.3.1$002fasjcl.2008.3.1.1071$002fasjcl.2008.3.1.1071.xml;jsessionid=F36717919BBF04391AC61CF44A516545

[2] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) доступна по адресу: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf .

- данные собираются в соответствии с целями обработки, обеспечивается их полнота и актуализация,
- использование данных для новых целей должно быть либо совместимо с первоначальной целью обработки, либо требуется согласие на новые виды использования или раскрытия информации,
- разумные меры безопасности для защиты данных, обеспечение подотчетности всех операторов данных,
- у субъекта персональных данных есть право на доступ к хранящимся о нём данным, а также право на их уничтожение или исправление.

Вместе с тем в новой редакции усиливаются требования к подотчётности оператора данных независимо от местонахождения данных, а также независимо от того, обрабатываются ли данные самим оператором, его представителями или передаются другому оператору.

ОЭСР рекомендует:

- использовать адаптированные под особенности организации программы управления защитой персональных данных и оценки последствий утечек для управления связанными с утечками рисками;
- включать в контракты положения, требующие соблюдения политики оператора данных по вопросам защиты персональных данных;
- устанавливать протоколы оповещения в случае инцидентов безопасности;
- разрабатывать план реагирования на инциденты безопасности и запросы со стороны субъекта персональных данных.

В настоящее время в число основных принципов защиты персональных данных входят:

1. **Принцип ограничения объема собираемых данных**

Объем собираемых персональных данных должен иметь пределы; все эти данные должны быть получены законным и честным образом – если возможно, то с ведома или согласия субъекта данных.

2. **Принцип качества данных**

Персональные данные должны соответствовать целям, в которых они будут использоваться; в той мере, в которой это необходимо в соответствии с упомянутыми целями, персональные данные должны быть точными, полными и регулярно обновляемыми.

3. Принцип конкретизации целей

Цели, в которых собираются персональные данные, должны быть конкретизированы не позднее момента сбора указанных данных, а их последующее использование должно ограничиваться достижением упомянутых либо сходных (совместимых) целей, которые должны указываться каждый раз, когда эти цели пересматриваются.

4. Принцип ограничений на использование данных

Персональные данные не должны разглашаться, предоставляться в пользование или иным образом использоваться в отличных от перечисленных в пункте 3 целях, за исключением случаев, когда:

a) субъект данных дает на то свое согласие;
b) это разрешено законом.

5. Принцип обеспечения безопасности

Персональные данные должны быть обеспечены должными механизмами защиты от рисков, связанных с потерей, несанкционированным доступом, уничтожением, использованием, изменением или разглашением данных.

6. Принцип открытости

Процесс развития, а также практика и политика в отношении персональных данных должны осуществляться в рамках общей политики открытости. В постоянной готовности должны быть средства для установления факта наличия и характера персональных данных, основных целей их использования, а также личности и обычного местонахождения распорядителя данных.

7. Принцип индивидуального участия

Индивидуум должен иметь право:

а) получать от распорядителя данных либо иным образом, подтверждения того, имеются ли у распорядителя данных персональные данные, относящиеся к упомянутому индивидууму;

б) получать относящиеся к нему персональные данные:

- в разумные сроки;
- если взимается плата, то по тарифу, не являющемуся чрезмерно высоким;
- в рамках разумной процедуры;
- в удобной для понимания форме;

в) в случае отказа от удовлетворения заявки, не предоставление информации, поданной в соответствии с пунктами (а) и (б), получать разъяснения о мотивах отказа и опротестовывать такой отказ;

г) опротестовывать относящиеся к нему данные; в случае удовлетворения протеста требовать того, чтобы таковые данные были уничтожены, исправлены или дополнены.

8. Принцип ответственности

Распорядитель данных должен нести ответственность за принятие мер, обеспечивающих соблюдение вышеперечисленных принципов. [1]

28 ЯНВАРЯ 2014 ГОДА В ОТМЕЧАВШИЙСЯ В ЕВРОПЕ ДЕНЬ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ВИЦЕ-ПРЕЗИДЕНТ ЕВРОПЕЙСКОЙ КОМИССИИ, УПОЛНОМОЧЕННЫЙ (ЕВРОКОМИССАР) ПО ВОПРОСАМ ЮСТИЦИИ ВИВИАН РЕДИНГ ВЫСТУПИЛА С РЕЧЬЮ, В КОТОРОЙ СФОРМУЛИРОВАЛА ВОСЕМЬ ПРИНЦИПОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, В СООТВЕТСТВИИ С КОТОРЫМИ ДОЛЖНА ОСУЩЕСТВЛЯТЬСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ КАК В ГОСУДАРСТВЕННОМ, ТАК И В ЧАСТНОМ СЕКТОРАХ.

Принцип 1: ***Европа должна создать надежную правовую базу*** для защиты персональных данных, которая могла бы стать для всего мира образцом и стандартом. В противном случае другие страны нас опередят и навяжут свои стандарты Европе.

Принцип 2***: Правовая база защиты персональных данных не должна проводить различие между частным и государственным секторами***. Граждане просто не поймут такое различие в условиях, когда государственный сектор собирает, сопоставляет, а иногда даже хочет продавать персональные данные.

Принцип 3. ***В ходе подготовки законодательства о защите персональных данных необходимо проводить его общественное обсуждение***, поскольку оно затрагивает гражданские свободы в онлайн-среде. Защита персональных данных должна быть темой кампании по информированию общественности,

---

[1] Рекомендации в отношении Руководящих принципов по защите неприкосновенности частной жизни и трансграничных потоков персональных данных» Организации экономического сотрудничества и развития (· OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) Доступно через: http://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en

направленной на совместное обсуждение вопроса гражданами, правозащитными группами, коммерческими компаниями и государственными органами.

Принцип 4: ***Ничем не ограниченный перехват электронных коммуникаций неприемлем***. Сбор данных в интересах наблюдения и контроля (surveilance) должен быть нацеленным и ограничен рамками, пропорциональными целям такого наблюдения.

Принцип 5: ***Законы должны быть четкими, и должна поддерживаться их актуальность.*** Нельзя, чтобы страны-члены Евросоюза, устанавливая рамки современных программ контроля и наблюдении, полагались на устаревшие законы, разработанные в другую технологическую эпоху. Такие законы мало или вообще ничего не говорят гражданам о том, что на самом деле происходит.

Принцип 6: ***Исключения со ссылкой на интересы национальной безопасности должны использоваться экономно***. Они должны быть именно исключениями, а не правилом. Необходимость защиты национальной безопасности может оправдать особые нормы. Однако не всё, что относится к внешним связям, является вопросами национальной безопасности. Иной подход подрывает легитимность законов, имеющих жизненно важное значение для нашей безопасности.

Принцип 7: ***Судебный надзор необходимо для того, чтобы избежать слишком сильного «раскачивания маятника» в разные стороны***. Надзор со стороны исполнительной власти – дело хорошее. Парламентский контроль необходим. Судебный же надзор является ключевым фактором.

Принцип 8: ***Законодательство о защите персональных данных должно применяться независимо от гражданства заинтересованных лиц***. Применение различных стандартов в зависимости от того, является ли лицо гражданином данной страны, не имеет никакого смысла ввиду открытой природы Интернета[1]

[1] Eecke, P. (2014) EUROPE: EU Commissioner Reding introduces her Eight Principles of Data Protection. Доступно через: http://www.jdsupra.com/legalnews/europe-eu-commissioner-reding-introduc-85150/

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Национальное законодательство

Первые законодательные акты в отношении персональных данных принимались в связи с созданием централизованных государственных баз данных уже в 1960-х гг. Однако нормы, принимавшиеся до 1970 г. носили, в основном, технический характер. В законах второй половины 1970-х гг. намного больше внимания уделялось правам индивидов. Третье поколение норм связано с реакцией на введение концепта «информационное самоопределение личности» в немецком законодательстве. Четвертое поколение норм связано с разработкой секторальных законов, дополняющих общие законы о защите персональных данных.

> В 1969 г. Парламент Великобритания принял «Билль о наблюдении за данными», устанавливающий контроль за собранной информацией. Первым целевым законодательным актом по защите персональных данных является немецкий Закон Земли Гессен 1970 года «О защите данных». Закон «О данных», принятый в Швеции в 1972 г. стал первым общенациональным законодательным актом,

Хотя процедурные нормы излагаются по-разному, в соответствии с правовой системой каждой страны, существует широкое согласие в отношении целей, которые должны быть обеспечены этими нормами. Национальные законодательства, включают, как минимум, следующие принципы, зафиксированные в международных документах:

- открытость – общество должно быть проинформировано о наличии баз персональных данных, которые находятся в распоряжении правительственных органов, организаций и учреждений;
- возможность доступа субъекта данных к данным о себе и возможность корректировать неточные или устаревшие данные;
- сбор персональных данных и объем этих данных должен быть ограничен в соответствии с целями сбора;
- ограничение использования – персональные данные должны использоваться только в целях, для которых они собирались;
- ограничения раскрытия – персональные данные могут быть раскрыты только в законных целях и с согласия субъекта данных[1].

[1] Bennett, C. Grant, R. (1999) Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press;

Рекомендации ОЭСР (2013)

Управление глобальными рисками требует разработки национальных стратегий стран с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных

- безопасность – данные должны быть защищены от потери, несанкционированного доступа, уничтожения, использования или модификации[1].

Национальные правовые системы защиты персональных данных могут основываться на двух принципиально отличающихся подходах:

- Генеральный – заключается в стремлении к созданию единого и всеобъемлющего закона о защите сферы частной жизни на основе права на невмешательство в частную жизни. Некоторые страны включили право на защиту персональных данных в Конституцию (Швеция, Бельгия, Греция, Нидерланды).
- Секторный (или отраслевой) – состоит в создании специализированных законов либо для каждого типа посягательств на сферу частной жизни, либо для каждой отрасли или сектора человеческой деятельности, являющейся потенциальным источником угроз для права человека на невмешательство в его частную жизнь (например, для почты и средств связи, для бюро кредитной информации, для средств массовой информации и рекламной сферы, для частных детективов, для компьютерных банков данных). Отраслевые законы представляют собой дополнительные законоположения, конкретизирующие положения базового национального закона о защите данных и обеспечивающие защиту персональных данных в отраслях человеческой деятельности, связанных с обработкой, передачей или использованием таких данных и несущих потенциальные угрозы посягательства на сферу частной жизни граждан. «Секторный» («отраслевой») подход, при котором новые «отраслевые» законы принимались по мере

[1] Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf

накопления прецедентной базы, указывающей на новый источник угроз для сферы частной жизни, приводил к бессистемности, дублированию и противоречивости законоположений.

Уже в конце 1990-х гг. эксперты отмечали, что в чистом виде и тот, и другой подходы оказались непродуктивными. В подавляющем большинстве стран современные национальные системы правового регулирования обработки и использования персональных данных применяют так называемый смешанный принцип, объединяющий определенные аспекты «генерального» и «отраслевого» подходов. Такой подход может быть эффективным только при наличии национальных стратегий стран с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных.

В странах-членах Европейского Союза в настоящее время ведется работа по модернизации регулирования защиты персональных данных.

Таблица 4. Ключевые изменения в рамках реформы законодательства стран-членов Европейского Союза в области защиты данных[1].

Общий свод правил защиты данных, действующий на всей территории ЕС. Ненужные административные требования, например, обязанность компаний направлять уведомления, будут отменены.
Вместо действующего сегодня требования, обязывающего все компании уведомлять органы по надзору за соблюдением защиты данных обо всех действиях по защите данных, регламентом предусмотрено повышение уровня ответственности и подотчетности лиц, осуществляющих обработку данных.
Компании и организации обязаны в максимально короткий срок (по возможности не позднее 24 часов) уведомлять национальный надзорный орган о серьезных нарушениях требований по защите данных.
Организации будут иметь дело только с одним национальным органом по защите данных в стране ЕС по месту основной регистрации. Аналогичным образом люди могут обращаться в орган по защите данных в своей стране, даже если обработку их данных осуществляет компания, находящаяся за пределами ЕС. Во всех случаях, когда требуется согласие на обработку данных, четко прописано, что такое согласие необходимо недвусмысленно получить, а не предполагать возможность его получения.

[1] European Commission (2012) Proposal for a regulation of the European parliament and of the Council щп the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Доступно через: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Право «быть забытым» поможет людям более эффективно устранять угрозу защите данных в сети интернет – им будет предоставлена возможность удалять свои данные, если нет законных оснований для их сохранения.
Компании, работающие на рынке ЕС и предлагающие свои услуги гражданам ЕС, будут обязаны при обработке данных за пределами ЕС руководствоваться правилами ЕС.
Независимые национальные органы по защите данных будут усилены, чтобы иметь возможность эффективнее добиваться соблюдения правил ЕС в своих странах. Они будут наделены полномочиями налагать штраф на компании, нарушающие правила ЕС в области защиты данных. Размер штрафных санкций может достигать €1 млн. или 2 % от суммы годового оборота компании.

Саморегулирование и со-регулирование

В отличие от многих других сфер управления специфика возникновения и развития интернета как распределенной, «саморегулирующейся» и «саморазвивающейся» сети не позволяет сводить вопросы упорядочивания соответствующих общественных отношений к формулированию «желательных» управляющих воздействий и их фиксации в виде норм права. Иначе говоря, управление путем принятия неких норм национального законодательства или международных соглашений абсолютно бесперспективно[1]. Поэтому саморегулирование в рамках интернет-бизнеса и различных организаций (в том числе и государственных) является одним из важнейших инструментов в политике защиты персональных данных. Связано это прежде всего с тем, что в ситуации быстрых технологических изменений, неопределённости отношений юрисдикций при трансграничной передаче персональных данных посредством глобальных телекоммуникационных сетей, национальное законодательство в принципе не в состоянии обеспечить надлежащий уровень информационной приватности человека.

Основные формы саморегулирования в сфере защиты персональных данных– это обязательства, кодексы, стандарты, корпоративные правила.

Основные формы саморегулирования – это обязательства, кодексы, стандарты, корпоративные правила.

[1] Курбалийя, Й. (2010)- Управление Интернетом. Доступно через: http://cctld.ru/files/IG-2010.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Мотивации саморегулирования в сфере защиты персональных данных можно суммировать следующим образом. Различные учреждения и институты посредством саморегулирования стремятся:

- избежать законодательных мер;
- предупредить разработку законодательных мер;
- заполнить пробелы в законодательстве;
- более эффективно реализовать нормы законодательства.

Инструменты саморегулирования могут разрабатываться на уровне:

- организации (государственной, частной, общественной, международной, национальной);
- сектора экономики;
- профессионального сообщества (например, для технических специалистов, которые занимаются обработкой информации, технологические кодексы предписывают определённые нормы для разного рода приложений).

Существуют различные пути принятия компаниями, организациями или отраслями мер саморегулирования в области защиты персональных данных:

> Обязательства (commitments) -это краткие констатации минимальных мер по защите персональных данных, обеспечение которых гарантирует та или иная организация (государственная, частная, общественная).

- информирование об обязательствах;
- введение внутренних руководящих указаний или принципов;
- принятие Кодексов практики или поведения;
- учреждение должности специального ответственного.

Обязательства – это краткие констатации минимальных мер по защите персональных данных, обеспечение которых гарантирует та или иная организация (государственная, частная, общественная).

Кодексы поведения – важнейший инструмент политики даже в тех странах, где существует достаточно эффективное законодательство, поскольку:

- позволяют организациям публично представить свою политику и обеспечить необходимую прозрачность с персональными данными;
- содействуют правильному применению мер, определённых законодательством;

Кодексы поведения – важнейший инструмент политики даже при наличии эффективного законодательства, поскольку

позволяют организациям публично представить свою политику и обеспечить необходимую прозрачность с персональными данными;

содействуют правильному применению мер, определённых законодательством;

процедура обсуждения кодексов содействует более глубокому пониманию проблем защиты персональных данных в различных сферах;

достаточно гибкие инструменты и легко могут изменяться с изменением технологических или экономических условий

- процедура обсуждения кодексов содействует более глубокому пониманию проблем защиты персональных данных в различных сферах;
- кодексы – достаточно гибкие инструменты и легко трансформируются с изменением технологических или экономических условий.

Директива ЕС от 24 октября 1995 о защите персональных данных выводит кодексы практики/поведения на международный уровень. В ст. 20 говорится:

«...страны-участницы должны поощрять заинтересованные деловые круги к участию в разработке европейских Кодексов поведения или профессиональной этики в отношении определенных отраслей деятельности на основе принципов, установленных в настоящей Директиве»[1].

В области защиты персональных данных форма, содержание и основная направленность кодексов практики/поведения не являются единообразными.

Анализ, проведенный ОЭСР, показывает, что в основе большинства кодексов лежит принцип «соблюдай или объясни». Пускай они, и содержат некоторые обязательные принципы, большинство рекомендаций по своей сути не носят обязательного характера и позволяют выбрать иной подход; в этом случае компании должны дать надлежащие объяснения[2].

Одним из ключевых элементов любого кодекса практики/поведения должен быть его добровольный характер. Соответственно, любой кодекс не предоставляет никаких законных прав другим сторонам, вовлеченным в процесс обработки, передачи и использования

[1] European Union. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Brussels: European Commission, OJ No. L281.24, October 1995

[2] Ваимерш, Э. (2013) Европейские кодексы корпоративного управления и их эффективность. Доступно через: http://www.oecd.org/daf/ca/2013OECDRussiaCorporateGovernanceRoundtableEuropeanCodesRus.pdf

Если кодекс поведения просто, провозглашает широкие принципы защиты данных, но не предлагает мер для соблюдения этих принципов, то такой кодекс не является средством защиты данных

персональных данных. Например, субъекты данных или лицо, передающее данные, не обретают никаких прав против держателя данных, который создал конкретный кодекс. Однако это не препятствует кодексу быть обязательным для исполнения внутри данной отрасли или корпорации. Например, нарушение отраслевых стандартов, содержащихся в кодексах, может привести к прекращению членства их нарушителя в соответствующей отраслевой или профессиональной ассоциации.

Если кодекс просто провозглашает широкие принципы защиты данных, но затем не предлагает мер для соблюдения этих принципов, то такой кодекс не является средством защиты данных.

Следует отметить, что кодексы поведения/практики являются обычно инструментами частного сектора. Этому способствуют несколько причин:

- регулирование защиты данных государственного сектора обычно осуществляется на основании правил, установленных внутренними инструкциями;
- в большинстве стран защита данных частного сектора остается сравнительно нерегулируемой, что предоставляет отраслям и корпорациям возможности для саморегулирования.

Исторически сложилось так, что многие кодексы ограничиваются рамками отдельных секторов бизнеса. Прежде всего, в банковской и страховой отраслях, поскольку именно здесь собирают огромные количества персональных данных и располагают технологическими возможностями для их обработки. Кроме того, эти отрасли могут быть внутренне взаимосвязаны через корпоративное право собственности и могут иметь интересы в смежных областях бизнеса

(например, службы безопасности торговли), тем самым потенциально способствовать еще большей концентрации данных. В рамках индустрии прямого маркетинга, строящегося на использовании информации о потребителях, создание кодексов практики/поведения также стало общепринятой практикой.

Существуют и межотраслевые кодексы. Национальный компьютерный центр Великобритании разработал ряд кодексов, относящихся к: (1) службам безопасности; (2) компьютерным бюро; (3) данным о наемных служащих; (4) управлению собственностью; (5) информации о потребителях и поставщиках.

Кодексы поведения в отношении защиты персональных данных имеют и международные организации. Свод практических правил Международной Организации Труда (International Laboui Organization- ILO) по защите персональных данных работника был принят на совещании экспертов в 1996 г. Кодекс не имеет обязательной силы, но может быть использован при разработке национального законодательства. В нем изложены основные принципы сбора, обработки, использования и хранения личной информации о работниках, а также о лицах, обращающихся к работодателю в целях трудоустройства. Специальные разделы Свода посвящены личным правам работника, возникающим в связи со сбором персональных данных, в частности, праву на уведомление о сборе персональных данных, на ознакомление в рабочее время со сведениями о себе, которые имеются у работодателя, на получение копий документов, право на доступ к медицинским документам через своего врача-представителя и др. Эти требования могут служить надежным ориентиром при принятии конкретных решений в отношении защиты личных данных работников и содействовать разработке соответствующего национального законодательства.

Как и законодательное регулирование, кодексы поведения имеют свои ограничения. Анализ достоинств и недостатков этой формы саморегулирования, проведенный ОЭСР, остается актуальным и сейчас.

Достоинства саморегулирования:

- кодексы поведения доказали, что они могут быть весьма гибкими инструментами для внедрения закона в конкретные отрасли и сектора экономики;
- релевантные процедуры обладают весьма позитивным воздействием на взаимосвязь палаты с различными отраслями и секторами экономики;
- и те, и другие ведут к улучшенному осознанию и пониманию проблем и вопросов защиты персональных данных, которые являются специфическими для каждой отрасли или сектора экономики;
- кодексы поведения предоставляют определенным отраслям удобную возможность продемонстрировать реальную заботу о вопросах защиты права на невмешательство в частную жизнь;

- отрасли и сектора, подлежащие регулированию кодексом, наделенным правовой санкцией, могут служить примером и посредником для других.

Недостатки саморегулирования:

- регулирование при помощи кодексов может быть ограничено условиями конкуренции и другими аспектами некоего конкретного сектора или отрасли;
- кодексы поведения могут усложнить или запутать правовые рамки, которые применяются в конкретном секторе или отрасли;
- субъекты данных не всегда осведомлены о статусе конкретного кодекса поведения: наделен он правовой санкцией или нет;
- требование адекватных консультаций может создать проблемы с поиском достаточно компетентного партнера;
- практический эффект любого кодекса может зависеть соответственно от сферы его компетенции и статуса, а также иных специфических условий[1].

Стандарты

Стандарты – это не только технические критерии надежности степени защиты персональных данных, но и инструменты реализации политики в этой сфере. Ведь стандартизация, по сути, представляет собой общепринятую процедуру оценки, которая позволяет определить, действительно ли организация делает то, что провозглашает в качестве правил, и включает три компонента:

- установление технических стандартов;
- установление стандартов процедур обработки (менеджмента);
- процедуры оценки влияния тех или иных технологий на защиту персональных данных[2].

Разработкой стандартов в этой сфере, наряду с Международной организацией стандартизации (ISO), занимается Европейский комитет по стандартизации (The Centre Européanne de Normalisations (CEN). Вместе с рабочей группой Article 29 они контролируют выполнение Директивы ЕС 1995 г., устанавливая и контролируя стандарты в трех сферах:

- общий стандарт защиты персональных данных (практические меры, которые организации должны реализовать для выполнения требований Директивы);
- секторальные стандарты (информация в сфере здравоохранения и пр.);

---

[1] OECD documents. Privacy and data protection: Issues and Challenges", Information Computer Communication Policy. Organization for Economic Cooperation and Development, Paris, 1966, p. 46 -47.

[2] ISO 22307:2008 on Financial Services: Privacy Impact Assessment (ISO 22307:2008 Финансовые услуги. Оценка влияния конфиденциальности); ISO 9564-1:2002, Banking–PIN Management and Security–Part 1: Basic Principles and Requirements for Online PIN Handling in ATM and POS Systems; ISO 18043:2006, Information Technology–Security Techniques–Selection, Deployment and Operations of Intrusion Detection Systems ИСО/МЭК 18043:2006 'Информационные технологии – Методы гарантии безопасности. Доступно через: http://vsegost.com/Catalog/57/5736.shtml

- стандарты для специфических задач (главным образом, в онлайновой среде).

Сертификация

Сертификация (получение сертификатов соответствия стандартам) конкретизирует требования и делает более продуктивной процедуру аудита и проверки на соответствие требованиям[1].

Оценка влияния на защиту персональных данных

Оценка влияния на защиту персональных данных – это, по сути, оценка возможных рисков. Ясные критерии оценки риска для защиты данных при введении тех или иных процедур частными и государственными учреждениями позволяют предупредить возможные нарушения законодательства, а общественности предусмотреть возможные угрозы информационной приватности.

Такая оценка должна осуществляться в соответствии с определёнными правилами и учитывать:

- тип персональных данных, которые подвергаются риску,
- источник, из которого будет получаться информация,
- обстоятельства сбора информации,
- процесс обработки персональных данных,
- предполагаемое использование имеющихся или производимых персональных данных,
- предполагаемых реципиентов и способы использования ими информации,
- обстоятельства, при которых производится информация,
- возможные условия использования и раскрытия информации,
- меры по недопущению неавторизованного доступа, раскрытия, модификации или уничтожения. [2]

---

[1] Winn, J. (2008) Technical Standards as Data Protection Regulation. Доступно через: http://dx.doi.org/10.2139/ssrn.1118542

[2] Bennett, C. (2001) What government should know about privacy: a foundation paper. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Технологии

К инструментам политики защиты персональных данных аналитики относят и технологии, обеспечивающие приватность на основе принципа «проектируемой конфиденциальности».

Заложенная при проектировании защита персональных данных (privacy by design) – это концепция, которая исходит из того, что защита личной информации, не может быть обеспечена исключительно соблюдением нормативно-правовых актов. Такая защита должна стать «правилом по умолчанию» в работе любой организации, что означает:

Заложенная при проектировании защита персональных данных (privacy by design) - это концепция, которая исходит из того, что. защита личной информации, не может быть обеспечена исключительно соблюдением нормативно-правовых актов. Такая защита должна стать «правилом по умолчанию» в работе любой организации

- **Встраивание конфиденциальности в конструкцию системы должно быть активным, а не ограничиваться лишь мерами по устранению последствий.** Личная информация должна быть защищена до того, как система запущена в работу, а не после выявления нарушений конфиденциальности.
- **Конфиденциальность как стандартная установка.** Параметры по умолчанию часто являются определяющими (многие пользователи вообще их никогда не меняют). Поэтому необходимо обеспечить максимальный «автоматизм» в той или иной информационной системе или деловых отношениях. Не требуется никаких действий со стороны индивидуума для защиты личной информации, — система уже изначально содержит в себе необходимые установки.
- **Конфиденциальность как часть структуры**. Защита личной информации должна стать неотъемлемой частью архитектуры любой информационной системы или деловых отношений.
- Полная функциональность с суммарным положительным результатом – **учет всех законных интересов и целей «беспроигрышным» способом, без ненужных компромиссов** (например, укрепление безопасности системы в противовес защите личной информации демонстрирует, что можно обеспечить и то, и другое).
- **Защита личной информации на протяжении всего цикла** ее сбора, хранения, обработки и уничтожения.
- **Доступность и открытость – гарантии того, что система действительно работает в соответствии с заявленными принципами и целями** (это должно быть подтверждено независимой проверкой). Все компоненты и операции остаются

открытыми и доступными, как для пользователей, так и для тех, кто обеспечивает сервис.

- **Соблюдение конфиденциальности пользователей**. Система должна быть ориентирована, в первую очередь, на пользователя: защита личной информации по умолчанию, своевременное уведомление о сборе личной информации, предоставление пользователю свободы выбора в удобной и понятной форме[1].

Наиболее распространённые технологические инструменты, обеспечивающие защиту персональных данных – это шифрование, технологии анонимизации и «псевдонимизации», фильтры.

Технологии, как и другие инструменты политики защиты персональных данных, имеют недостатки. Прежде всего, пользователю иногда бывает сложно узнать или понять, правильно ли работает технология. Можно заметить сигналы нарушения приватности: сомнительные электронные сообщения, появление персональной информации в интернете и пр. Но вряд ли возможно с абсолютной уверенностью утверждать, что с технической точки зрения приватность обеспечена. Более того, даже если ошибки и сбои обнаруживаются и исправляются специалистами, обычно сложно узнать, внесены ли изменения технически корректным способом.

Просвещение

Законы, кодексы, технологический дизайн не в состоянии обеспечить защиту персональных данных, если индивиды не умеют предотвратить вмешательство в цифровую сферу частной жизни. Информирование и образование граждан – важный инструмент в работе регулирующих органов, неправительственных организаций, политических партий. Однако просвещение в сфере защиты персональных данных – это не только обучение технологиям, но и пропаганда социальных норм, ответственного поведения в отношении как своих данных, так и информации о других.

РЕЗЮМЕ

Политика в отношении персональных данных имеет многоуровневый и кросс-секторальный характер. В нее вовлечены наднациональные, национальные и субнациональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Только серьёзный анализ таких кластеров

[1] Кавукиан, Э. (2011) Privacy by Design 7 основополагающих принципов. Доступно через: http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-russian.pdf

интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий.

Набор инструментов политики в отношении защиты персональных данных включает не только меры законодательного регулирования, но и транснациональные принципы, руководства и соглашения, практики саморегулирования, стандартизации, технологические решения и просветительские мероприятия. Закон должен дополняться кодексами поведения и технологическими мерами, опираться на соответствующую организационную культуру и поддержку общественности.

Управление глобальными рисками информационной приватности требует:

- соблюдения принципов законности, конкретизации целей, минимизации сбора и использования персональных данных, контроля субъекта данных, ответственности распорядителя данных и обеспечения безопасности данных;
- *разработки национальных стратегий* с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных;
- *подотчётности оператора (распорядителя, контролера) данных* независимо от местонахождения данных, а также независимо от того, обрабатываются ли данные самим оператором, его представителями или передаются другому оператору.

В ходе подготовки законодательства о защите персональных данных необходимо проводить его общественное обсуждение, поскольку оно затрагивает гражданские свободы в онлайн-среде. Защита персональных данных должна быть темой кампании по информированию общественности, направленной на совместное обсуждение вопроса гражданами, правозащитными группами, коммерческими компаниями и государственными органами.

Правовая база защиты персональных данных не должна проводить различие между частным и государственным сектором. Граждане просто не поймут такое различие в условиях, когда государственный сектор собирает, сопоставляет, а иногда даже хочет продавать персональные данные.

Исключения со ссылкой на интересы национальной безопасности должны использоваться экономно. Они должны быть именно исключениями, а не правилом. Необходимость защиты национальной безопасности может оправдать особые нормы. Однако не всё, что относится к внешним связям, является вопросом национальной безопасности. Иной подход подрывает легитимность законов, имеющих жизненно важное значение для нашей безопасности.

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

В сфере защиты персональных данных надзора со стороны исполнительной власти недостаточно. Необходим парламентский и судебный контроль.

Правозащитники и гражданские активисты, наряду с представителями государственных органов и бизнеса, могут и должны быть активными участниками диалога о стратегиях, приоритетах и балансе в сфере защиты персональных данных

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БЕЛАРУСИ

Защита персональных данных в Беларуси

МЕЖДУНАРОДНЫЕ ИНСТРУМЕНТЫ

Статья 17 Международного Пакта о гражданских и политических правах устанавливает, что «никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища, или тайну его корреспонденции, или незаконным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». Из этого базового, неотчуждаемого права на неприкосновенность личной жизни вытекает право индивида на защиту персональных данных.

Руководящие принципы ООН по регламентации компьютеризированных картотек, содержащих данные личного характера (1990 г.) требуют соблюдения следующих норм:

- любое лицо, удостоверяющее свою личность, имеет право знать, подвергаются ли касающиеся его данные обработке, получать об этом сообщение в понятной соответствующих исправлений в данные или уничтожение их в случае их незаконной, необоснованной или неточной регистрации и, если эти данные сообщались кому-либо, знать их получателя (ст.4);
- в любом законодательстве должен быть указан орган, который должен гарантировать соблюдение принципов беспристрастности, независимости по отношению к лицам или органам, ответственным за их обработку и применение, а также техническую компетентность (ст. 8).

В *Резолюции Генеральной ассамблеи ООН «Право на приватность в цифровую эпоху»* (2014) отмечается, что правительства должны:

- соблюдать международные нормы в области прав человека, когда они осуществляют прямой перехват частных коммуникаций или требуют у компаний предоставления персональных данных граждан;
- обеспечить доступ к эффективным механизмам урегулирования для тех, чьи права нарушены вследствие незаконной слежки и прочих самоуправных действий.

Особо оговаривается, что речь идет не только о содержимом интернет-коммуникаций, но и о сборе метаданных, которые могут включать временные метки email-сообщений или продолжительность телефонных звонков.

Республика Беларусь не присоединилась к Конвенции Совета Европы 108, которая представляет собой международный признанный стандарт в сфере защиты качества использования и защиты прав персональных данных.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БЕЛАРУСИ

НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО

Конституционные основы защиты персональных данных создают статьи 28 (гарантирует право на защиту гражданина от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство) и статья 34, часть 3 .(пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав) Конституции Республики Беларусь.

Основу политики в отношении персональных данных составляют закон «Об информации, информатизации и защите информации», закон «О регистре населения», закон «О переписи населения»

Что защищает закон

Определения термина «персональные данные» содержатся в законе «Об информации, информатизации и защите информации» и в законе «О регистре населения».

Практически все эксперты обращают внимание на то, что «определения, которые содержатся в законе «О регистре населения» и в законе «Об информации, информатизации и защите информации» имеют разный объем содержания. Если определение, содержащееся в законе о регистре населения, является исчерпывающим, то закон об информации относит к персональным данным любые данные, позволяющие идентифицировать лицо. Такая несогласованность ключевого определения приводит к невозможности единообразного подхода к правовому регулированию этой сферы».[1]

Таблица 5. Определение термина «персональные данные№ в законах Республики Беларусь

ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ»	ЗАКОН «О РЕГИСТРЕ НАСЕЛЕНИЯ».
персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения (ст.1)	персональные данные физических лиц (далее - персональные данные) - совокупность основных и дополнительных персональных данных, а также данных о реквизитах документов, подтверждающих основные и дополнительные персональные данные конкретных физических лиц

[1] Черных, Д (2014) Проблема использования и защиты персональных данных (рукопись)

иные данные, позволяющие идентифицировать такое лицо (ст.1) - открытый список	перечисление данных, которые могут быть отнесены к основным (ст. 8) и вспомогательным (ст. 10) персональным данным – закрытый список

Регистр определяется как «государственная централизованная автоматизированная информационная система, основу которой составляет база персональных данных граждан Республики Беларусь, а также иностранных граждан и лиц без гражданства, постоянно проживающих в Республике Беларусь (физических лиц) (Закон о регистре населения ст.2).

В Республике Беларусь законодательное выделение особо чувствительных/уязвимых категорий информации отсутствует и адекватной защиты им не предоставляется. Даже в пояснениях к закону о регистре населения, которые предложены Национальным центром законотворческой деятельности термин «чувствительные/ уязвимые данные» не употребляется.

«В регистре не будет никаких сведений, которые могут быть использованы для какого-либо давления на человека:

- о расе, национальности и цвете кожи;
- о мировоззрении, политических или религиозных убеждениях;
- о каких-либо заболеваниях;
- о сексуальной ориентации;
- об усыновлении и многие другие»[1].

Следует также отметить, что закон Республики Беларусь от 13.07.2006 N 144-З «О переписи населения» использует термин «персональные данные» в специальном значении, а именно как первичные статистические данные о конкретном респонденте, сбор которых осуществляется при проведении переписи населения, и предусматривает, что персональные данные являются конфиденциальными, не подлежат распространению (разглашению), в том числе представлению в государственные органы и иные организации, и используются исключительно для формирования итоговых данных.

Очевидно, что эти основополагающие законодательные акты содержат различающиеся определения. В формулировке закона «Об информатизации» термин «персональные данные» определяется не на основании сущностных признаков, а (1) через себя самое («персональные данные – это … персональные данные»); (2) через действия, которые над ними производятся.

---

[1] Аскерко, А. (б.г.) Комментарий к Закону Республики Беларусь «О регистре населения. Доступно через: http://www.center.gov.by/article61.html

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БЕЛАРУСИ

В законах «Об информации, информатизации и защите информации» и «О регистре населения содержатся» противоречивые трактовки термина «персональные данные»

Законодательное выделение особо чувствительных/уязвимых категорий персональных данных отсутствует и меры адекватной защиты таких данных не предусмотрены.

В итоге предлагаемая законодателем трактовка:

- не определяет «природу» персональных данных как информации, подвергающейся обработке (автоматизированными компьютерными системами и неавтоматизированными системами регистрации документов);
- не фиксирует сущностный признак персональных данных: «информация носит персональный характер, если можно установить (не обязательно на основании только этой информации) к кому конкретно она относится, другими словами, если субъекта можно идентифицировать на основании данной информации и эта информация относится именно к нему»[1].

Кого защищает закон?

Закон об информации, информатизации и защите информации – основной законодательный акт, касающийся персональных данных и их защиты, не содержит общих принципов обеспечения прав субъектов персональных данных.

Цель защиты персональных данных определяется в законе «О регистре населения» как предотвращение несанкционированного вмешательства в процесс ведения регистра, в том числе попыток незаконного доступа к персональным данным, содержащимся в регистре, их блокирования, копирования, предоставления, распространения, искажения, уничтожения, а также иных неправомерных действий в отношении этих персональных данных. Закон «Об информации, информатизации и защите информации» определяет цели защиты информации в целом (ст. 27).

Целями защиты информации являются:

- обеспечение национальной безопасности, суверенитета Республики Беларусь;

[1] Подробно об этом см.: http://www.lawtrend.org/ru/content/about/news/monitoring-izmenenii-zakon-ob-informacii/

В беларусских законодательных актах не содержится положений, которые включали бы все принципы защиты персональных. данных, перечисленные в 108 Конвенции Совета Европы.

- сохранение и неразглашение информации о частной жизни физических лиц и персональных данных, содержащихся в информационных системах;
- обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;
- недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Как защищает?

Закон «О регистре населения» требует принятия мер защиты данных с момента:

- когда персональные данные были предоставлены физическим лицом к которому они относятся,
- когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь,
- до уничтожения данных либо до получения согласия на разглашение данных (закон «Об информации, информатизации и защите информации»). Однако меры по защите персональных данных в законе не определены.

Отдельными нормативными правовыми актами регламентируется порядок доступа к информации о личной жизни граждан, порядок защиты информации, лицензирования деятельности по технической защите информации, в том числе:

- Декретом Президента Республики Беларусь от 14 июля 2003 г. № 17 «О лицензировании отдельных видов деятельности» (в части лицензирования деятельности по технической защите, в том числе

криптографическими методами, включая применение электронной цифровой подписи);

- Положением о лицензировании деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, утвержденном постановлением Совета Министров Республики Беларусь от 20 октября 2003 г. № 1374;
- Постановлением Комитета государственной безопасности Республики Беларусь от 12 декабря 2003 г. № 23 «Об организации выдачи специальных разрешений (лицензий) на осуществление деятельности, связанной с криптографической защитой информации и средствами негласного получения информации»;
- Инструкцией о режиме доступа к документам, содержащим информацию, относящуюся к тайне личной жизни граждан, утвержденной приказом Комитета по архивам и делопроизводству Республики Беларусь от 3 июля 1996 г. № 21.

Как закон «Об информации, информатизации и защите информации», так и закон «О регистре населения» закрепляют один из основных принципов обработки персональных данных – получение согласия физического лица, к которому относятся персональные данные, на любое действие с персональными данными, кроме случаев, когда получение такого согласия не требуется в соответствии с законодательными актами (ст. 18 закона «Об информации, информатизации и защите информации»).

Как закон «Об информации, информатизации и защите информации», так и закон «О регистре населения» закрепляют один из основных принципов обработки персональных данных – получение согласия физического лица, к которому относятся персональные данные, на любое действие с персональными данными.

Статьи 18, 32,34 закона «Об информации, информатизации и защите информации», в которых речь идет о письменном согласии физического лица на сбор, обработку и хранение его/ее персональных данных и о праве «пользователя информации» знакомиться со своими персональными данными, отсылают к случаям, установленным иными законодательными актами Республики Беларусь.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БЕЛАРУСИ

В законе «О регистре населения» указывается, что форма письменного заявления о предоставлении персональных данных из регистра определяется распорядителем регистра. Письменное согласие физического лица может выражаться путем:

- оформления нотариально удостоверенной доверенности на получение персональных данных из регистра;
- нотариального свидетельствования подлинности подписи на заявлении физического лица (его законного представителя) о согласии на получение персональных данных о нем из регистра;
- удостоверения уполномоченным сотрудником регистрирующей службы заявления физического лица (его законного представителя) о согласии на получение персональных данных о нем из регистра (пункт 6 статьи 26 Закона «О регистре населения»).

Единый подход к регламентации факта фиксации обращения за персональными данными законодательство не предусматривает. Закон «О регистре населения» закрепляет каждый факт обращения к персональным данным, содержащимся в регистре населения, фиксируется в онлайн-режиме. В отношении персональных данных, которые содержатся в других базах данных, такого требования на законодательном уровне нет[1].

В белорусских законодательных актах не содержится положений, которые включали бы все принципы защиты персональных данных, перечисленные в 108 Конвенции Совета Европы. Исключение составляет Соглашение между Правительством Республики Беларусь и Правительством Финляндской Республики о сотрудничестве и взаимной помощи в таможенных делах.

В частности, в национальном законодательстве отсутствует единый подход к срокам хранения персональных данных. Если в международном правовом регулировании устанавливается необходимость лимитировать по времени хранения таких данных (на срок, необходимый для достижения какой-либо цели их хранения), то в беларусском законодательстве сроки хранения персональных данных могут тянуться вплоть до смерти гражданина[2].

Исследования Д. Черных (РПОО «Белорусский Хельсинкский Комитет»), проанализировавшего правовую регламентацию функционирования девяти общенациональных баз данных, показали, что:

- разумный срок хранения данных (срок, необходимый для достижения цели хранения данных) предусмотрен только для двух баз данных (Автоматизированная информационная система «Расчет» и «Персонифицированный учет»),

[1] Черных, Д. (2014) Проблема использования и защиты персональных данных физических лиц (рукопись)
[2] Там же

- субъект персональных данных фактически не может узнать, кто получал доступ к его данным (законодательное регулирование в этой части отсутствует либо неконкретное),
- четкое определений целей сбора и хранения разработано только для 5 из 9 баз данных,
- принцип минимизации сбора данных соблюдается для 7 из 9 баз[1].

Доступ к персональным данным регламентируется в законе Республики Беларусь «О переписи населения» и в законе Республики Беларусь «О регистре населения».

Согласно закону «О регистре» все организации условно делятся на 2 группы:

- организации, для которых использование персональных данных из регистра необходимо для выполнения задач, входящих в компетенцию этих организаций, определенную законодательством Республики Беларусь,
- организациям, для которых использование персональных данных из регистра не является необходимым условием выполнения их задач, будут предоставляться только обезличенные персональные данные и только на платной основе.

Организациям первой группы данные предоставляются бесплатно по договору о регулярном предоставлении данных (посредством удаленного доступа или на бумажных носителях). Каждая из этих организаций имеет доступ к строго ограниченному сегменту персональных данных физических лиц. Перечень показателей для обмена информацией определяется договором о регулярном предоставлении персональных данных из регистра, фиксируется в протоколе обмена и автоматически обеспечивается при обмене информацией. Организация-получатель информации из регистра имеет идентификационный код (ключ авторизации, электронная цифровая подпись), который включается во все информационные сообщения данной организации. А регистр населения с помощью системы распознавания ключей автоматически определяет, что и в каком объеме можно выдавать организации-получателю и что от нее получать.

Организации, не нуждающиеся в регулярном получении данных из регистра, смогут получить их по письменному или электронному запросу без заключения договора. При этом они смогут получить лишь ограниченный перечень персональных данных, необходимый для выполнения задач, предусмотренных их компетенцией.

Второй группе организаций предоставляются только обезличенные персональные данные и только на платной основе. Эти организации не имеют доступа к регистру и данные получают только по соответствующим образом оформленному запросу.

---

[1] Черных, Д. (2014) Обеспечение законодательного регулирования защиты персональных данных на примере некоторых баз данных, аккумулирующих персональные данные (рукопись)

Общедоступных массивов персональных данных в регистре нет. Любые данные из регистра будут выдаваться только при авторизованном доступе и строго в объеме, определенном правами конкретной организации-получателя.

Порядок доступа к информации о личной жизни граждан регулируется отраслевыми законодательными актами (инструкции о режиме доступа к документам, содержащим информацию, относящуюся к тайне личной жизни граждан, утвержденной приказом Комитета по архивам и делопроизводству Республики Беларусь от 3 июля 1996 г. № 21 и т.п.).

Физические лица могут получать персональные данные из регистра населения на основании Постановления Министерства внутренних дел Республики Беларусь от 22.11.2012 № 410, которым установлена форма письменного заявления о предоставлении персональных данных физических лиц, в котором указывается ФИО лица, данные о котором запрашиваются, его идентификационный номер и документы, подтверждающие право на получение информации.

Во всех остальных случаях, когда персональные данные лица получаются не из регистра населения, следует руководствоваться общей нормой ст.18 Закона «Об информации, информатизации и защите информации», которая устанавливает необходимость получения согласия лица на передачу его данных. Однако форма и процедура подобных действий в законодательстве не установлена.

В беларусском законодательстве нет специальных мер ответственности за незаконное распространение и использование персональных данных. Соответствующие незаконные деяния могут повлечь административную либо уголовную ответственность.

Административная ответственность. Статья 22.6 Кодекса Республики Беларусь об административных правонарушениях[1] устанавливает ответственность за несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, – в виде штрафа в размере от 20 до 50 базовых величин. Статья 22.7 предусматривает целый ряд составов административных правонарушений за нарушение правил защиты информации.

Уголовная ответственность наступает за:

- незаконный сбор либо распространение информации о частной жизни (ст. 179 Уголовного кодекса Республики Беларусь[2], далее – УК);
- хищение путем использования компьютерной техники (ст. 212 УК);

---

[1] Кодекс Республики Беларусь об Административных Правонарушениях 194-З от 21.04.2003 г. http://etalonline.by/?type=text&regnum=Hk0300194#load_text_none_1_

[2] Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1_

- несанкционированный доступ к компьютерной информации (ст. 349 УК);
- изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) (ст. 350 УК);
- умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) (статья 351);
- неправомерное завладение компьютерной информацией (ст. 352 УК).

На практике могут возникать трудности при квалификации противоправных деяний за разглашение персональных данных по данным составам. В этой связи необходимо внесение дополнения в законодательство Республики Беларусь, предусматривающих ответственность за противоправное распространение и использование персональных данных.

Таким образом, детальный порядок работы с персональными данными, их сбора, обработки, хранения законодательными актами не определен, в том числе:

- процедура подготовки и направления запроса на предоставление персональных данных;
- процедура получения согласия субъекта персональных данных на распространение или предоставление персональных данных третьим лицам.

Не содержит действующее законодательство Республики Беларусь и классификации персональных данных, что также вызывает неправильное и неполное понимание сущности и правовой природы персональных данных в Республике Беларусь.

Положения закона «О регистре населения» и нормы, содержащиеся как в действующем законе «Об информации, информатизации и защите информации», относятся только к действиям государства в лице уполномоченных органов в отношении данных физических лиц, содержащихся в регистре населения. В законе Республики Беларусь «Об информации, информатизации и защите информации» и других упомянутых выше законодательных и нормативных актах, связанных с оборотом персональных данных, определяется лишь порядок и правовые основы действий определенных государственных органов, ведущих регистр с персональными данными. Во всех остальных случаях – например, при получении персональных данных юридическими лицами при ведении коммерческой деятельности – данные при обработке, передаче и иных действиях остаются незащищенными на должном уровне. При такой постановке вопроса закон не регулирует и не защищает персональные данные физических лиц при их получении, обработке, хранении, передаче и уничтожении иными субъектами.

Таким образом, беларусское законодательство в сфере защиты персональных данных характеризуются, прежде всего, тем, что:

- не содержит единообразного определения «персональных данных»;
- не регулирует ситуации «объединения данных» (профайлинг);
- не соответствует требованиям 108 Конвенции Совета Европы[1];
- государственные органы и организации практикуют различные стандарты сбора, хранения и обработки персональных данных;
- в нормативных правовых актах, регламентирующих функционирование различных баз данных, отсутствуют единообразные подходы к установлению сроков хранения персональных данных;
- у граждан отсутствует возможность знать кто, когда и с какой целью собирает их персональные данные, кто обращается к их персональной информации, хранящейся в государственных базах данных;
- отсутствует четкая регламентация сбора, хранения, обработки и использования персональных данных коммерческими структурами.

ТЕХНИЧЕСКИЕ СТАНДАРТЫ И СЕРТИФИКАТЫ

Технические стандарты и сертификаты информационной безопасности – это второй по значимости (после законодательства) инструмент политики в отношении защиты персональных данных.

Правовые и организационные основы оценки соответствия объектов оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации определяет закон Республики Беларусь от 5 января 2004 года «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации». Данный документ направлен на обеспечение единой государственной политики при осуществлении оценки соответствия. Общие требования к порядку проведения обязательной и добровольной сертификации отечественной и импортируемой продукции устанавливает технический кодекс установившейся практики ТКП 5.1.02-2012 «Национальная система подтверждения соответствия Республики Беларусь. Сертификация продукции. Основные положения».

В соответствии с Указом Президента Республики Беларусь от 16.04.2013 N 196 «О некоторых мерах по совершенствованию защиты информации», утвердившим нормы технической и криптографической защиты информации, обязательные для применения собственниками (владельцами) информационных систем, в которых обрабатывается служебная информация ограниченного распространения, информация о частной жизни физического лица и персональные данные. Целью защиты информации является:

- предотвращение несанкционированного доступа к информации;

[1] См. раздел «Международные принципы»

- несанкционированного воздействия на информацию.

В числе мер защиты информации фиксируются:

- определения перечня объектов защиты;
- обеспечение проведения мероприятий по созданию систем защиты информации;
- подтверждение соответствия систем защиты информации требованиям законодательства об информации, информатизации и защите информации (аттестация систем защиты информации);
- методическое руководство деятельностью по применению мер технической защиты информации;
- представление сведений в Оперативно-аналитический центр о состоянии технической защиты информации;
- криптографическая защита информации.

При осуществлении технической защиты информации используются средства защиты, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром.

Республиканский орган управления в сфере стандартизации – Государственный комитет по стандартизации (Госстандарт). Органом сертификации систем информационной безопасности является подразделение Госстандарта – Белорусский государственный институт стандартизации и сертификации (БелГИСС). Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ) аккредитован Национальным органом по аккредитации Республики Беларусь в качестве органа по сертификации средств защиты информации и продукции по требованиям безопасности информации. Сертификация систем менеджмента информационной безопасности осуществляется в Национальной системе подтверждения соответствия Республики Беларусь. Зарегистрирована со статусом наблюдателя в объединенном техническом комитете ISO/IEC JTC 1.

Система стандартизации включает:

- стандарты серии 34.101 (Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий). Стандарты устанавливают общие подходы к формированию требований и оценке безопасности информационных технологий, определяют виды требований безопасности и содержат их систематизированный каталог, критерии и уровни оценки безопасности информационных технологий, позволяющие оценить правильность реализации средств безопасности, стойкость механизмов защиты, использования отечественной нормативной базы.

- стандарты по криптографической защите информации — СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования», применяемые при разработке средств криптографической защиты.

Стандарты первой группы разрабатываются на основе международных стандартов, что обеспечивает международное признание беларусских сертификатов. Однако необходимость непрерывного отслеживания и внедрения международной нормативной базы приводит к отставанию в принятии и использовании стандартов на 3-5 лет[1].

Непосредственное отношение к защите прав субъектов персональных данных имеет стандарт ISO 26000 «Руководство по социальной ответственности», рабочей группой ISO/TMB «Социальная ответственность», в 2010 г., активным членом которой (до ее расформирования по окончании разработки стандарта) являлась Республика Беларусь.

Представители бизнес-сообщества обращают внимание на ряд проблем, связанных с утвердившимися в Беларуси подходами к стандартизации в сфере обеспечения информационной безопасности, в том числе на то, что:

- стремление обеспечить ИБ «один раз и навсегда»,
- требования ИБ устанавливаются «сверху-вниз» без учета реальных потребностей бизнеса,
- проводится политика унификации требований ИБ для совершенно различных отраслей бизнеса и госсектора,
- стремление обеспечить 100% безопасность.

Причины этих проблем кроются в том, что:

- отсутствует диалог государства и бизнеса,
- экономической составляющей информационной безопасности отведена второстепенная роль,
- отсутствует системность,
- игнорируются лучшие мировые практики[2].

Решение этих проблем связано с ориентацией на стандарты:

- «Цели контроля для информационных и смежных технологий» (COBIT),
- «Библиотека ИТ инфраструктуры при Управлении правительственной коммерции Великобритании» (ITIL),

---

[1] Жук, О.(2009) Нормативно-правовое обеспечение информационной безопасности в системах электронного документооборота. Доступно через: http://media.miu.by/files/store/items/uses/xviii/mim_uses_xviii_13011.pdf

[2] Базелев, В (2012) Реализация требований регуляторов в области информационной безопасности в соответствии с мировыми практиками. Доступно через: http://infopark.by/sites/default/files/file_attach/bazelev_luchshie_praktiki_ib_bevaleks.pdf

Отсутствие надлежащей законодательной базы – одна из основных причин того, что в Беларуси нет организаций саморегулирования, которые могли бы обеспечить защиту персональных данных. Даже информирование об обязательствах («правила приватности») не рассматриваются в качестве обязательного элемента деятельности предприятий и организаций

- стандарты ISO серии 27000 по информационной безопасности,
- требования к системе управления качеством ISO 9001:2000.

Так, в 2013 г. был вручен первый сертификат на систему менеджмента информационной безопасности по СТБ ISO/IEC 27001 (разработка стандартов этой серии была завершена в 2005 г.).

С 1 января 2014 г. был введен в действие технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденный постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375, а также вступает в силу (и вступил в действие приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY).

САМОРЕГУЛИРОВАНИЕ

Задача снижения административного давления на бизнес и создания условий для активизации частной инициативной деятельности граждан, поставленная Директивой Президента Республики Беларусь от 31 декабря 2010г. №4, выдвигает на повестку дня вопросы дальнейшей либерализации экономики и сокращения регулятивных функций государства. Поэтому важным составным элементом реализации стратегии экономического развития страны становится внедрение механизмов саморегулирования предпринимательской деятельности. При этом речь не идет об ослаблении роли государства, а о сокращении его вмешательства в экономические процессы[1]. «Поэтому использование

[1] Совет по развитию предпринимательства Республики Беларусь (2014) Саморегулирование бизнеса как условие эффективного развития экономики. Доступно через: http://ced.by/ru/publication/books/~shownews/samoregulirovanie-biznesa

института саморегулирования как альтернативного государственному регулированию способа преодоления провалов рынка требует определения условий, при которых развитие саморегулирования возможно и оправдано с точки зрения интересов участников рынка и общественных интересов»[1].

В целях реализации этого пункта мероприятий в 2011 году, созданной при Министерстве юстиции рабочей группой, подготовлена первоначальная редакция проекта закона Республики Беларусь «О саморегулируемых организациях». Этот закон должен был стать рамочным, определяющим общие нормы для саморегулирования во всех сферах экономической деятельности, где данный институт будут вводиться. В августе 2011 г. документ был передан на согласование в Министерство экономики Республики Беларусь. В работу были вовлечены представители различных государственных органов. Поскольку законопроект напрямую затрагивал интересы бизнеса, в рабочей группе были широко представлены предпринимательские союзы и ассоциации. Но так сложилось, что проект «не пошел». Ситуацию не спас предложенный со стороны предпринимательских структур альтернативный вариант документа. Не давалось ответов на главные вопросы: в каких сферах возможно введение саморегулирования и каков правовой механизм его реализации.

В связи с актуальностью рассматриваемой темы, сохранением к ней интереса со стороны бизнес-сообщества было принято решение о целесообразности подготовки концепции соответствующего законопроекта. Данное решение содержалось в указе Президента от 3 января 2013 г. № 1. «Об утверждении плана подготовки законопроектов на 2013 год».

Заявлялось, что в концепции будет предложен анализ законодательства, в том числе международных договоров Республики Беларусь, относящегося к предмету правового регулирования проекта, обзор научных исследований, публикаций в печати, законодательства иностранных государств, иметь предварительную структуру законопроекта, содержать прогноз финансово-экономических и иных возможных последствий его принятия. При этом подготовленный вариант концепции должен был быть согласован с заинтересованными органами и организациями, а на последней стадии — с главой государства[2].

Концепция в соответствии с планом была представлена палате представителей в 2013 г. В документе, в частности, отмечается, что отдельных положений, касающихся саморегулирования, закреплённых в отдельных отраслевых законодательных актах, для введения института саморегулируемых организаций, недостаточно.

[1] Крючкова П., Шаститко А. Развитие саморегулирования бизнеса и государственное вмешательство в экономику

[2] Юнчик, Л (2013) Первый проект «не пошел» http://www.pravo.by/main.aspx?guid=100573

Внедрение механизмов саморегулирования требует реализации комплекса мер, которые можно разбить на два блока:

- меры, направленные на формирование институциональных условий;
- меры, касающиеся оптимального построения схемы саморегулирования.

К первому блоку можно отнести следующие меры:

а) законодательное определение направлений взаимодействия государственных органов и саморегулируемых организаций;

б) развитие отраслевого законодательства, предполагающего передачу определенных функций государственных органов саморегулируемым организациям (в отраслевом законодательстве должно содержаться определение функций и полномочий саморегулируемых организаций):

- четкое определение функций саморегулируемых организаций в целях исключения возможности «двойного регулирования» определенной сферы;
- создание возможности появления в конкретной сфере нескольких конкурирующих между собой саморегулируемых организаций;
- установление запрета на определенные действия саморегулируемой организации, которые могут ограничить конкуренцию, в том числе, путем создания барьеров входа на рынок;
- выработка требований по транспарентности и информационной открытости саморегулируемых организаций, включая информацию о требованиях, составе членов организации, системе разрешения споров, порядку принятия решений, результатов рассмотрения жалоб и др.;
- разработка стандартов по разрешению споров и по возможным формам участия третьих лиц в функционировании саморегулируемых организаций и в мониторинге за деятельностью этих организаций;

в) постепенное снижение уровня административного давления на экономику путем поэтапного отказа государства от функций регулирования в отдельных сферах в пользу саморегулируемых организаций;

г) продвижение идеи саморегулирования – активная государственная политика, направленная на просвещение профессионального сообщества и поддержку институтов саморегулирования.

Саморегулируемые организации разрабатывают и устанавливают обязательные для выполнения всеми членами саморегулируемых организаций правила и стандарты предпринимательской деятельности, согласованные с уполномоченным государственным органом (далее – правила и стандарты саморегулируемых организаций). Правила и стандарты саморегулируемых организаций должны соответствовать актам законодательства. Правила и стандарты саморегулируемой

организации устанавливают дополнительные требования к деятельности членов саморегулируемой организации[1].

Однако проект концепции не был упомянут и в плане внесения на обсуждение Палатой представителей на 2014 г[2]. Отсутствие надлежащей законодательной базы – одна из основных причин того, что в Беларуси нет организаций саморегулирования, которые могли бы обеспечить защиту персональных данных. Даже информирование об обязательствах («правила приватности») не рассматриваются в качестве обязательного элемента деятельности предприятий и организаций.

Из 64 провайдеров, предоставляющих доступ в интернет (список сайта providers.by), только 7 компаний так или иначе информируют клиентов о политике приватности.

На сайтах трех провайдеров размещена информация о том, что они действуют в сфере защиты персональных данных в соответствии с нормами беларусского законодательства. Еще три провайдера разместили тексты типовых договоров, содержащих пункт об обязательствах провайдера в отношении конфиденциальности.

На сайте компании Velcom можно найти пункты о защите персональных данных в довольно объемном Кодексе поведения Telekom Austria Group. (http://www.velcom.by/ru/documents/ru/Kodeks_Povedeniya.pdf)

Таблица 6. Кодекс поведения Telekom Austria Group

Кодекс поведения Telekom Austria Group
4.2.1 Защита данных **Мы осознаем важность и конфиденциальность персональных данных, доверенных нам нашими клиентами, сотрудниками, акционерами и поставщиками, и делаем все возможное для их защиты. Каждый в Telekom Austria Group несет ответственность за сохранение конфиденциальности в рамках выполняемых задач.** **Мы собираем и обрабатываем персональные данные только с разрешения вовлеченного лица, если это разрешено законом и необходимо для исполнения контрактных или правовых обязательств. Более того, мы собираем, обрабатываем и используем персональные данные только в необходимой**

[1] Министерство юстиции РБ (2013) Концепция проекта закона Республики Беларусь «О саморегулируемых организациях». Доступно через: http://tinyurl.com/pv7fb2b

[2] Национальное собрание Республики Беларусь. Палата представителей. Планы подготовки законопроектов. Доступно через: http://house.gov.by/index.php/,7034,,,,0,,,0.htm

степени и для заданных целей. Мы уважаем всесторонние права тех людей, информацию о которых мы собираем, обрабатываем или используем.

4.2.2 Сохранность данных

Сохранность данных имеет большое значение для Telekom Austria Group. Данный аспект существенно влияет на успешность нашего бизнеса и репутацию компании. Поэтому мы охраняем информацию о компании так же тщательно, как и личные данные наших клиентов и сотрудников, применяя все имеющиеся и подходящие технические и организационные средства для предотвращения несанкционированного доступа и использования или злоупотребления, потери и преждевременного уничтожения.

ПРОСВЕЩЕНИЕ

В Республике Беларусь не проводилось никаких кампаний, и нет государственных образовательных программ, направленных на повышение осведомленности граждан в сфере защиты персональных данных. В 2014 г. Центр правовой трансформации разработал учебник «Защита персональных данных: введение в проблематику» и организовал онлайновый курс «Защита персональных данных: теория, история, практика».

Некоторая косвенная информация сообщалась в рамках Дня безопасного интернета, который стал отмечаться в Беларуси с 2013 года.

Между тем потребность в получении информации по этой проблематике достаточно высока. Так большинство респондентов исследования ЦЕТ-Центра правовой трансформации сообщили о необходимости получения дополнительных знаний и компетенций, связанных с защитой персональных данных.

Таким образом, гражданские активисты вполне серьёзно обеспокоены проблемой защиты персональных данных, имеют отдельные сведения о специфике этого вопроса (иногда разрозненные и несистематичные, иногда очень глубокие) и, что самое важное, заинтересованы в получении дополнительных знаний и компетенций:

- представители общественных организаций достаточно самокритично оценивают свой уровень осведомленности в сфере защиты персональных данных, одновременно обозначая потребность в получении дополнительных знаний и компетенций в этой сфере.
- невысоко оценивают функциональную грамотность беларусских граждан по вопросам защиты персональных данных участники фокус-групп.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БЕЛАРУСИ

В силу непрозрачности системы государственного управления в Беларуси, довольно трудно сделать вывод о соблюдении ими прав субъектов персональных данных. Вместе с тем, показателен факт, что нормы закон не требуют публикации на сайтах государственных органов обязательств в отношении защиты персональных данных тех, кто пользуются этими ресурсами.

КТО ОБЕСПЕЧИВАЕТ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ?

Правительство?

Законодатели и органы государственного управления – основные акторы, регулирующие защиту персональных данных в Республике Беларусь. Независимого экспертного органа, контролирующего качество защиты данных и гарантии прав субъектов данных в стране, нет.

В статье 30. закона «Об информации, информатизации и защите информации» говорится о том, что защита информации организуется «в отношении общедоступной информации – лицом, осуществляющим распространение и (или) предоставление такой информации; в отношении информации, распространение и (или) предоставление которой ограничено, – собственником или оператором информационной системы, содержащей такую информацию, либо обладателем информации, если такая информация не содержится в информационных системах; иными лицами в случаях, определенных настоящим Законом и иными законодательными актами Республики Беларусь».

Субъекты защиты персональных данных прямо не поименованы. В законе выделены лишь субъекты информационных отношений в общем: владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей, информационный посредник, обладатель информации, оператор информационной системы, пользователь информации, пользователь информационной системы и (или) информационной сети, собственник программно-технических средств, информационных ресурсов, информационных систем

и информационных сетей. В законе «О регистре населения» названы следующие субъекты:

распорядитель регистра и регистрирующая служба как структурное подразделение распорядителя регистра, уполномоченное на ведение регистра.

В соответствии с законом «О регистре населения», ответственность за надлежащее внесение данных в регистр несут те организации, которые вносят данные. Ответственность за адекватную обработку и хранение данных несет распорядитель регистра – Министерство внутренних дел. Надзор за точным и единообразным исполнением законодательства Республики Беларусь в сфере функционирования регистра осуществляют Генеральный прокурор Республики Беларусь и подчиненные ему прокуроры (Закон о регистре населения, ст. 34).

Закон «О регистре населения» предусматривает, что органом, ответственным за ведение регистра населения, содержащего персональные данные, является МВД. Одновременно и другие органы ведут свои ресурсы, в которых содержатся определенные данные (Нацбанк осуществляет хранение кредитных историй физических лиц, Фонд социальной защиты населения – данных государственного социального страхования)[1].

В силу непрозрачности системы государственного управления в Беларуси, довольно трудно сделать вывод о соблюдении ими прав субъектов персональных данных. Вместе с тем, показателен факт, что нормы закона не требуют публикации на сайтах государственных органов обязательств в отношении защиты персональных данных тех, кто пользуются этими ресурсами. В качестве примера корректной политики приведем сообщение о политике конфиденциальности на сайте Президента Российской Федерации.

Таблица 7. Сайт президента РФ: политика приватности

Сайт Президента РФ: политика приватности
Уважаемые посетители! **1. При использовании информации, размещаемой на официальном интернет-сайте Президента России (далее – Сайт), технические средства Сайта автоматически распознают сетевые (IP) адреса и доменные имена каждого пользователя (посетителя Сайта). Упомянутые сведения; электронные адреса лиц, пользующихся интерактивными сервисами Сайта и (или) отправляющих электронные сообщения в адреса, указанные на Сайте; автоматически накапливаемые сведения о том, к каким интернет-страницам Сайта обращались пользователи; иные сведения (в том числе персонального характера),**

[1] Черных, Д. (2014) Проблема использования и защиты персональных данных физических лиц (рукопись)

сообщаемые пользователями, – хранятся с использованием технических средств Сайта для целей, перечисленных в пункте 2 настоящего Уведомления.

2. Сведения о пользователях Сайта, накапливаемые и хранимые в технических средствах Сайта, используются исключительно для целей совершенствования способов и методов представления информации на Сайте, улучшения обслуживания его пользователей (посетителей), выявления наиболее посещаемых интернет-страниц (интерактивных сервисов) Сайта, а также ведения статистики посещений Сайта.

3. Вне пределов, указанных в пункте 2 настоящего Уведомления, информация о пользователях Сайта не может быть каким-либо образом использована или разглашена. Доступ к таким сведениям имеют только лица, специально уполномоченные на проведение работ, указанных в пункте 2 настоящего Уведомления, и предупрежденные об ответственности за случайное или умышленное разглашение либо несанкционированное использование таких сведений.

4. Информация персонального характера о пользователях Сайта хранится и обрабатывается с соблюдением требований российского законодательства о персональных данных.

5. Какая-либо информация, являющаяся производной по отношению к сведениям, перечисленным в пункте 1 настоящего Уведомления, представляется для последующего использования (распространения) исключительно в обобщенном виде, без указания конкретных сетевых (электронных) адресов и доменных имен пользователей (посетителей) Сайта.

6. Рассылка каких-либо электронных сообщений по сетевым (электронным) адресам пользователей (посетителей) Сайта, а также размещение на Сайте гиперссылок на сетевые (электронные) адреса пользователей Сайта и (или) их интернет-страницы допускаются исключительно, если такая рассылка и (или) размещение прямо предусмотрены правилами использования соответствующего интерактивного сервиса и на такую рассылку и (или) размещение получено предварительное согласие пользователя (посетителя) Сайта, выраженное в форме, предусмотренной указанными правилами. Переписка с пользователями (посетителями) Сайта, не относящаяся к использованию интерактивных сервисов Сайта либо иных информационных разделов Сайта, не производится

Бизнес?

Как отмечалось выше, законодательство Республики Беларусь концентрируется, главным образом, на защите персональных данных, которые находятся в распоряжении государственных органов. Требования к бизнес-структурам заключаются, прежде всего, в технических стандартах информационной безопасности и отраслевых нормативных актах.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БЕЛАРУСИ

> *Законы Республики Беларусь концентрируется, главным образом, на защите персональных данных, которые находятся в распоряжении государственных органов. Требования к бизнес-структурам заключаются, прежде всего, в технических стандартах информационной безопасности и отраслевых нормативных актах*

Как и следовало ожидать, с наибольшим вниманием к этому относятся банки, которые концентрируют свои усилия на технических аспектах защиты персональных данных[1].

Степень осознания представителями бизнеса необходимости защищать персональные данные иллюстрируют приводимые ниже высказывания участников фокус-групп:

- *«Так как я работаю с базами данных, соответственно это персональные данные о фирмах или ком-либо. Это регулируется очень просто: во-первых, есть ограниченный круг людей. Во-вторых, я ответственен за эту информацию. Если я кому-то что-то разглашу, то я буду уже уголовно ответственный. Все просто. Выбор зависит от меня»;*
- *[Когда вы определяете, что правильно, а что нет, то на какие нормы вы ориентируетесь?] «Личное понимание, основанное на знании законов»;.*
- *«Пользователи прекрасно представляют, зачем нужны эти данные. Наши пользователи нигде не ставят галочку, что они против того, что их данные предоставляют рекрутерам…. Вот появится организация-конкурент у нас и скажет, что не будет предоставлять данные рекрутерам. Но такого конкурента у нас нет»;*
- *«Лучший способ [защиты данных] это квалификация пользователя, который сам следит за этим и думает какие данные и кому он предоставляет. Существует возможность для государства оценить, что такой-то процент населения не умеет пользоваться сетью интернет и их очень легко одурачить. И, что бы не утекали банковские номера, проще просто запретить собирать эти данные».*

Анализ высказываний респондентов показал два плана представления о персональных данных. Первое понятие о персональных данных обсуждается в контексте рекламных и, шире, бизнес-стратегий с использованием интернет-сервисов. В этом контексте понятие

[illegible]ких банков [Обзор состояния, тенденций и перспектив развития [illegible]нологий в Республике Беларусь в 2013году] Взгляд банков Республики [illegible]пно через: http://www.bankit.by/files/2014/analitika/otchet-banki-2013.pdf

персональных данных трактуется максимально широко. Два «модальных» высказывания по этому поводу следующие:

- к персональным данным относится все, что связано с личностью и ее действиями (читать следует как «с личностью в интернете»), то есть все фактологические данные о человеке, его интересы, история посещения сайтов, покупок, высказанных мнений и т.п.;
- что считать персональными данными, определяется в каждой конкретной ситуации.

Представления о границах законности использования информации о личности основывались на наивно-априорных представлениях о человеческом благе. Если мы используем эту информацию, чтобы продать что-то дороже или ненужное человеку – это плохо, а если для того, чтобы предложить ему скидки или то, что ему будет реально полезно – то это хорошо и правильно.

Другое, более узкое, представление о персональных данных актуализируется, когда разговор заходит о практике собственной компании по работе с ними. Тогда появляются определения, что «это данные, которые можно связать с конкретной физической личностью», «данные, которые если куда-нибудь утекут, могут нанести тебе вред», и т.п. Как показывают ответы респондентов, в большинстве случаев фирмы и компании имеют некие внутренние регламенты и правила по работе с персональными данными, однако строгость этих регламентов и усилия, предпринимаемые для защиты персональных данных, весьма различны. Иногда эти вопросы решаются опосредованием работы с персональными данными почтовыми или иными сервисами, которые являются одновременно и сборщиком, и ответственным за хранение персональных данных, а компания имеет дело с вполне конкретной информацией о пользователе, но не привязанной к «физической личности». В некоторых компаниях имеется ограниченный список людей, получающих

Исследование Центра правовой трансформации и ЦЕТ, ноябрь-декабрь 2014

Тех, кто хочет, чтобы их права, связанные с пользованием интернета, были гарантированы, в три раза больше чем тех, кто хочет понимать и принимать участие в обсуждении того, как и кем будут гарантированы эти права

доступ к базам данных клиентов или партнеров, и устанавливаются строгие нормы по обращению с данными.

В целом, ответы на вопрос, на что ориентируются участники фокус-группы в работе с персональными данными, можно объединить в три группы:

- некодифицированные нормы – правила морали, профессиональная этика, представления о том, «что такое хорошо и что такое плохо» и т.п.;
- политика и нормативные стандарты компании или информационного ресурса;
- беларусское законодательство рассматривается как основание для возможной апелляции по отношению к общим нормам по защите чести и достоинства и невмешательстве в частную жизнь.

Другие акторы?

Продвижение и защита права на неприкосновенность частной жизни согласуется с миссией правозащитного сообщества, с используемыми методами работы. Правозащитные организации понимают суть проблем обеспечения неприкосновенности частной жизни, вооружены набором готовых универсальных критериев, деятельно настроены на изменение ситуации. Но большая часть правозащитных организаций не относит решение вопросов защиты и продвижения права на неприкосновенность частной жизни к числу приоритетных задач. Отчасти потому, что миссия эта сложна для освоения, проблемы не связаны напрямую с политическим произволом власти, нарушения часто скрыты от поверхностного взгляда, для многих являются обыденным, обычным явлением. Для решения предложенных задач нужно прилагать дополнительные усилия, чтобы:

- фиксировать нарушения цифровой приватности в повседневной жизни,

- объяснять смысл происходящего (законодательное регулирование, международные инициативы и т.п.),
- формировать эффективные и гибкие подходы к взаимодействию с органами власти.

Беларусский Хельсинкский Комитет, Центр правовой трансформации уже проделали значительную работу в этом направлении. Анализ законодательства, просветительская деятельность, обзоры и рекомендации, подготовленные экспертами этих организаций, создали необходимый базис для информированного обсуждения политики в отношении защиты персональных данных в Беларуси[1].

Исследование ЦЕТ-Центра правовой трансформации показывает, что для журналистов проблематика защиты персональных данных не актуализирована. В своей работе они опираются на некоторые представления о вмешательстве в частную жизнь, а также на закон «О защите чести и достоинства», а в качестве практически единственного ориентира в повседневной работе пользуются представлениями о журналистской этике. Журналисты, освещающие политическую деятельность, акции оппозиционных партий и активистов, используют инструменты «анонимизации» информации об активистах и их действиях, даже взятой из открытых источников, и именно это относится респондентами к сфере работы с персональными данными.

Дискуссии в фокус-группах показали, что журналисты не видят себя в качестве субъекта решения данной проблемы. Рекомендации по работе с проблемой защиты персональных данных от респондентов-журналистов связаны в основном с «повышением уровня грамотности населения», введения неких «элементарных предметов» в школах, ВУЗах. Причины этого заключаются в традиционных установках большинства беларусских СМИ:

- «средства массовой информации удовлетворяют спрос населения, а спроса населения на эту тему нет»;
- для того, чтобы тема присутствовала в СМИ, нужны «информационные поводы» (в качестве таковых были названы возможные скандалы или реальные факты о существенных финансовых потерях, связанных со злоупотреблением персональными данными, судебные разбирательства по этому поводу).

---

[1] Свободный интернет: политические принципы и правовые нормы: Республика Беларусь в глобальном контексте. Доступно через: http://tinyurl.com/ntl7rjk; 2nd cycle Universal Periodic Review of the Republic of Belarus. Submitted on 15 September 2014. Доступно через: http://www.belhelcom.org/sites/default/files/UPR_Belarus_Alternative%20report_en.pdf и др.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БЕЛАРУСИ

Необходим диалог

Результаты социологического исследования, проведённого Центром правовой трансформации совместно с ЦЕТ в ноябре-декабре 2014 г. показали, что ценность неприкосновенности частной жизни онлайн и защиты персональных данных по своей важности занимает второе место после свободного обмена информацией. Две трети гражданских активистов высказались за это. При этом, в праве на открытый и прозрачный процесс принятия решений относительно функционирования сети, ограничения со стороны беларусского государства чувствует только половина гражданских активистов (19 из 40). Другими словами, тех, кто хочет, чтобы их права, связанные с пользованием интернета, были гарантированы, в три раза больше чем тех, кто хочет понимать и принимать участие в обсуждении того, как и кем будут гарантированы эти права.

На вопрос о том, кто должен заниматься обсуждением и реализацией принципов свободного интернета в Беларуси (сообщалось, что в число этих принципов входит и защита информационной приватности), большинство интервьюируемых (94%) ответило: «Это должна быть совместная работа всех заинтересованных сторон».

Наличие двух обозначенных выше несовместимых установок свидетельствует о том, что первоочередной задачей с точки зрения обеспечения надлежащей защиты прав субъектов персональных данных является инициирование широкого общественного диалога.

РЕЗЮМЕ

В Беларуси все острее становится проблема по обеспечению прав граждан по защите неприкосновенности их частной жизни, персональных данных, что обусловлено:

- использованием новых технологий,
- ростом киберпреступности,
- стремлением спецслужб контролировать сферы активной деятельности граждан.

Практически единственными инструментами политики по отношению к защите персональных данных в Республике Беларусь являются законодательство и разработка технических стандартов.

Конституционные, законодательные нормы, регулирующие в Беларуси право на неприкосновенность частной жизни, на практике слабо гарантируют защиту данного права.

- Законодательство Республики Беларусь определяет лишь общие вопросы защиты персональных данных (без четкого механизма их реализации), а также

точечно регулирует отдельные сферы, в которых используются персональные данные.

- Беларусские законодатели придерживаются «отраслевого» подхода: базовый закон в данной сфере отсутствует, а меры регулирования устанавливаются по мере накопления прецедентной базы, указывающей на источник угроз, что приводит к бессистемности и дублированию законоположений, рассредоточенности норм по различным отраслям права и аспектам общественных отношений.
- Неурегулированными остаются вопросы ответственности за неправомерное разглашение персональных данных. На сегодняшний день отсутствуют специальные составы за незаконное распространение и использование персональных данных.
- Беларусское законодательство не соответствует международным стандартам. Республика Беларусь - одно из немногих государств, которое не подписало и не ратифицировало Конвенцию Совета Европы о защите физических лиц при автоматической обработке персональных данных от 28 января 1981 года.

Отечественные правоведы утверждают, что насущной задачей является совершенствование законодательства о персональных данных и, прежде всего, разработка и принятие закона либо концепции защиты персональных данных. [1]

Необходимый баланс между юридическими и административными инструментами отсутствует.

Низкий уровень осведомленности граждан и слабое знание об ответственности в сфере использования персональных данных у представителей бизнеса обуславливает необходимость просветительских и образовательных компаний.

Решение сложных и взаимосвязанных задач невозможно без широкого общественного диалога.

[1] Шугай, А. (2013) Некоторые проблемы защиты персональных данных в Республике Беларусь; Конституция Республики Беларусь 1994 года с изм. и доп.: текст по состоянию на 1 августа 2011 г. – Минск: Амалфея, 2011. – 48 с.;. О регистре населения: Закон Респ. Беларусь от 21 июля 2008 г. № 418-З: текст по состоянию на 12 мая 2012 г. – Право и экономика, 2012. – 12 с.;3. О переписи населения: Закон Респ. Беларусь от 13 июля 2006 г. № 144-З: текст по состоянию на 23 апр. 2012 г. – Минск: Амалфея, 2012. – 4 с.; Об информации, информатизации и защите информации: Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З: текст по состоянию на 20 янв. 2012 г. – Минск: Амалфея, 2012. –14 с.; Кодекс Республики Беларусь об административных правонарушениях: принят Палатой представителей 17 дек. 2002 г.: одобрен Советом Респ. 2 апр. 2003 г.: текст Кодекса по состоянию на 1 марта 2012 г. – Минск: ИООО «Право и экономика», 2012. – 149 с.; Уголовный кодекс Республики Беларусь: принят Палатой представителей 2 июня 1999 г.: одобрен Советом Респ. 24 июня 1999 г.: текст Кодекса по состоянию на 29 нояб. 2011 г. – Минск: ИООО «Право и экономика», 2011. – 273 с.; Солдатенко, В.А. Правовое регулирование вопросов защиты персональных данных в Республике Беларусь и иностранных государствах / В.А. Солдатенко // КонсультантПлюс: Беларусь [Электронный ресурс] / ООО «ЮрСпектр». – Минск, 2012.

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

Заключение и рекомендации

На начальных этапах использования автоматизированных систем обработки данных о гражданах, проблема регулирования представлялась узко-юридической задачей: разработать регламент сбора, хранения и обработки таких данных, обязанности и права сторон и т.п.

Однако переход от «банков данных» к децентрализованным информационным системам, размывание различий между частным и государственным сектором (аутсорсинг, сбор данных) и распространение разнообразных технологий мониторинга и контроля потребовали разработки целого набора политических инструментов. Вместе с тем, стало очевидным, что проблема защиты персональных данных носит комплексный характер и при ее решении необходимо учитывать и структурные факторы: бюрократизацию организаций, глобализацию и развитие технологий

Защита персональных данных перестала быть проблемой, понимание которой доступно только технической элите и юристам, специализирующимся в сфере информационного права. Сейчас она обсуждается на национальном и на глобальном уровне политиками, юристами и техническими специалистами, представителями бизнеса и общественными активистами.

В основе публичной политики в отношении персональных данных лежит рациональное убеждение о том, что политические принципы и нормы права могут обеспечить защиту от рисков, которые появляются с развитием новых технологий. Структурными элементами является совокупность программ и приоритетов органов власти и государственного управления, механизмов и технологий реализации программ такой политики.

➢ **Регулирование защиты персональных данных в Беларуси представляет собой фрагментированный набор норм и правил, которые во многих случаях не соответствуют международным стандартам и не обеспечивают надлежащей защиты качества данных и прав субъектов данных.**

Уже сейчас можно говорить о необходимости:

- *разработки единой стратегии, концепции или кодекса защиты персональных данных,*
- *создания единого экспертного органа по защите прав субъектов персональных данных,*
- *расширения репертуара инструментов политики (в том числе поощрение саморегулирования, принятие закона о саморегулировании),*
- *введения обязательной оценки влияния на приватность,*
- *гармонизации беларусского законодательства с международными принципами и нормами,*

- *повышения ответственности органов государственного управления и бизнеса.*
    - **Закон – самый важный инструмент регулирования, но он должен быть гибким. Принципы закона должны быть специфицированы в других инструментах.**
    - **Разработка политики в отношении персональных данных и внедрение стандартов и правил должны проходить в режиме консультаций с представителями бизнеса, общественных организаций и технического сообщества.**

Правительство не может не принимать в расчет ожидания и систематические действия других акторов. Уровень политической поддержки или популярности той или иной позиции важен для структуры «баланса» между приватностью, защитой прав субъектов персональных данных и безопасностью.

Поскольку консенсус в этом отношении не достигнут пока даже на теоретическом уровне, решение задачи защиты персональных данных – это непростой процесс анализа последствий с учетом интересов различных сторон в конкретной ситуации. При этом никакое решение не может быть окончательным. А широкое общественное обсуждение должно стать гарантией того, что новые вызовы и возможности ответов на них в достаточной степени учитываются при разработке стратегий.

- **Ключевым условием такого диалога является просвещение и повышение осведомленности как граждан, «субъектов персональных данных», так и распорядителей данных (государственных органов и коммерческих организаций).**
- **Диалог всех заинтересованных сторон о способах реформирования существующего в Беларуси режима политики в отношении защиты персональных данных может фокусироваться на следующих вопросах:**

- *набора основополагающих принципов защиты персональных данных*

Ясный набор принципов приватности должен использоваться как основа будущего регулирования и руководство для государственных органов.

- *рационализации и усовершенствования подходов к регулированию защиты персональных данных с учетом*
    - *приоритета защиты граждан как стороны, обладающей наименьшими возможностями по защите своих персональных данных при взаимодействии с бизнесом и государством.*

Поскольку в вопросе защиты персональных данных в интернете интересам граждан противостоят интересы государства и бизнеса, обладающих большими возможностями по отстаиванию своей точки зрения, реальный баланс будет соблюден лишь в том

случае, когда государством будут предоставлены исполнимые гарантии защиты персональной информации граждан.

- *важности поддержки саморегулирования и рыночных механизмов.*

Развитие интернета не требует активного вмешательства со стороны государства, большинство ключевых вопросов развития всемирной паутины решаются в порядке саморегулирования. При проведении регулирования обращения персональных данных в интернете, необходимо оценивать положительные и отрицательные последствия, неизбежно следующие за любым нормативным урегулированием. При этом государство может способствовать формированию и развитию добросовестных обычаев обращения с персональными данными.

- *минимизации препятствий добросовестной коммерческой деятельности*

При введении новых норм, связанных с обращением персональных данных, важно оценивать их влияние на деятельность лиц, ведущих добросовестную коммерческую деятельность, в том числе на поставщиков интернет-услуг и владельцев веб-сайтов. Необходимо сопоставлять выгоды, приобретаемые от регулирования, с негативными последствиями, прежде всего, экономического характера.

- *прозрачность деятельности органов государственной власти, например, за счет информирования о:*
  - количестве запросов,
  - числе и списке организаций, имеющих доступ,
  - статистическом числе операций консультирований о получении доступа,
  - статистическом числе операций извлечения персональных данных.

➢ **Важный ресурс реформирования – опыт, накопленный в этой сфере государствами Европейского Союза и станами–членами Совета Европы.**

Библиография

1. Агапеева, К. (2012) Теория секьюритизации Барри Бузана. Доступно через: http://www.geopolitica.ru/article/teoriya-sekyuritizacii-barri-buzana#.VG2uO_msXzc
2. Ариков, Г. (2014) Аспекты неприкосновенности частной жизни в уголовном законодательстве Республики. Доступно через: http://www.cnaa.md/files/theses/2014/26884/gheorghii_aricov_abstract_ru.pdf
3. Аскерко, А. (б.г.) Комментарий к Закону Республики Беларусь «О регистре населения. Доступно через: http://www.center.gov.by/article61.html
4. Базелев, В (2012) Реализация требований регуляторов в области информационной безопасности в соответствии с мировыми практиками. Доступно через: http://infopark.by/sites/default/files/file_attach/bazelev_luchshie_praktiki_ib_bevaleks.pdf
5. Ваимерш, Э. (2013) Европейские кодексы корпоративного управления и их эффективность. Дступно через: http://www.oecd.org/daf/ca/2013OECDRussiaCorporateGovernanceRoundtableEuropeanCodesRus.pdf
6. Директива N 95/46/EC Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных». Ст. 8 Доступно через: http://books.ifmo.ru/file/pdf/1570.pdf
7. Жук, О.(2009) Нормативно-правовое обеспечение информационной безопасности в системах электронного документооборота. Доступно через: http://media.miu.by/files/store/items/uses/xviii/mim_uses_xviii_13011.pdf
8. Зиновский В. (2014) Информационное общество в Республике Беларусь, 2014. Доступно через: http://belstat.gov.by/bgd/public_compilation?id=520
9. EDRI (2012) Защита персональных данных. Введение». Доступно через: http://www.lawtrend.org/information-access/zashhita-dannyh
10. Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html
11. Инфопарк, Ассоциация белорусских банков [Обзор состояния, тенденций и перспектив развития банковских информационных технологий в Республике Беларусь в 2013году] Взгляд банков Республики Беларусь на ИТ-технологии. Доступно через: http://www.bankit.by/files/2014/analitika/otchet-banki-2013.pdf
12. ИСО/МЭК 18043:2006 'Информационные технологии - Методы гарантии безопасности. Доступно через: http://vsegost.com/Catalog/57/5736.shtml
13. Кавукиан, Э. (2011) Privacy by Design 7 основополагающих принципов. Доступно через: http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-russian.pdf
14. Крючкова П.В., Шаститко А.Е. (2004) Развитие саморегулирования бизнеса и государственное вмешательство в экономику. Доступно через: http://www.budgetrf.ru/Publications/Magazines/bea/bulletin/2004/bea592004bull/bea592004bull000.htm
15. Кодекс Республики Беларусь об Административных Правонарушениях 194-З от 21.04.2003 г. http://etalonline.by/?type=text&regnum=Hk0300194#load_text_none_1_

БИБЛИОГРАФИЯ

16. Конституция Республики Беларусь 1994 года с изм. и доп.: текст по состоянию на 1 августа 2011 г. Минск: Амалфея
17. Красотенко, О.Ю. Понятие «частная жизнь» в решениях Европейского Суда по правам человека. Минск, 2011. Доступно через: http://elib.bsu.by/handle/123456789/29040
18. Курбалийя, Й. (2010). Управление Интернетом. Доступно через: http://cctld.ru/files/IG-2010.pdf
19. Мельников, М. В. (2012) О семантике понятия "приватное" // XIII международная научная конференция преподавателей, аспирантов и студентов НСИ. С.181-189
20. Министерство юстиции РБ (2013) Концепция проекта закона Республики Беларусь «О саморегулируемых организациях». Доступно через: http://tinyurl.com/pv7fb2b
21. Национальная программа ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы. Постановление Совета Министров Республики Беларусь, 28 марта 2011 г. № 384. Доступно через: http://www.mpt.gov.by/File/Natpr/natpr_19_03_2014.pdf
22. Национальное собрание Республики Беларусь. Палата представителей. Планы подготовки законопроектов. Доступно через: http://house.gov.by/index.php/,7034,,,,0,,0.htm
23. Паризер, Э. (2012) За стеной фильтров. Что интернет скрывает от нас. Москва, Альпина
24. Прохвачева, О.Г. (2000) Лингвокультурный концепт "приватность": На материале американского варианта английского языка. Доступно через: http://www.dissercat.com/content/lingvokulturnyi-kontsept-privatnost-na-materiale-amerikanskogo-varianta-angliiskogo-yazyka#ixzz3AMsvTYM
25. Рекомендация МСЭ-Т X.1205, Обзор кибербезопасности. Доступно через: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru
26. Свободный интернет: политические принципы и правовые нормы: Республика Беларусь в глобальном контексте. Доступно через: http://tinyurl.com/ntl7rjk; 2nd cycle Universal Periodic Review of the Republic of Belarus. Submitted on 15 September 2014. Доступно через: http://www.belhelcom.org/sites/default/files/UPR_Belarus_Alternative%20report_en.pdf.
27. Совет по развитию предпринимательства Республики Беларусь (2014) Саморегулирование бизнеса как условие эффективного развития экономики. Доступно через: http://ced.by/ru/publication/books/~shownews/samoregulirovanie-biznesa
28. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1_
29. Шахов Н.И. (2008) Отношения по охране частной жизни и информации о частной жизни как объект теоретико-правового исследования. Ростов-на Дону. С. 7
30. Шугай, А. (2013) Некоторые проблемы защиты персональных данных в Республике Беларусь. Доступно через: http://pravo.by/Conf2012/reports/Shuhai.doc
31. Черных, Д (2014) Проблема использования и защиты персональных данных. Доступно через: http://belhelcom.org/ru/node/19699
32. Юнчик, Л (2013) Первый проект «не пошел» http://www.pravo.by/main.aspx?guid=100573
33. APC (2013) A cyber security agenda for civil society: what is at stake? Доступно через: http://www.apc.org/en/pubs/cyber-security-agenda-civil-society-what-stake

34. Bennett, C. (2001) What Government Should Know about Privacy: A Foundation Paper. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf
35. Bennett, C. (2008) The Privacy Advocates: Resisting the Spread of Surveillance. Cambridge, MA: MIT Press;
36. Bennett, C. Grant, R. (1999) Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press
37. Bennett, C. and Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge, MA: The MIT Press
38. Bernard A. La protection de l'intimité par la droit privé: eloge du ragot ou comment vices exposes engendrent vertu. Les For Interieur, p.153-179. Доступно через http://www.u-picardie.fr/labo/curapp/revues/root/35/alain_bernard.pdf_4a081e8ad4544/alain_bernard.pdf
39. BS 7799-3:2006.Standard on Information Security Management Systems–Guidelines for Information Security Risk Management. Доступно через: http://www.iso.staratel.com/ISO17799/Doc/BS7799.3.1999/BS%207799-3-2006.pdf
40. Buzan,B., Waever, O. Wilde, J. (1998) Security: A New Framework for Analysis. Доступно через:http://books.google.by/books/about/Security.html?id=j4BGr-Elsp8C&redir_esc=
41. Bygrave, L. (2010) Privacy and data protection in an international perspective. Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf
42. Bygrave, L. (2002) Data Protection Law: Approaching its Rationale, Logic and Limits. The Hague: Kluwer Law International
43. Data Insight (2014) Какие тренды на белорусском рынке e-commerce в этом году, Доступно через: http://probusiness.by/markets/154-kakie-trendy-na-belorusskom-rynke-e-commerce-v-etom-godu.html
44. Eecke, P. (2014) EUROPE: EU Commissioner Reding introduces her Eight Principles of Data Protection. Доступно через: http://www.jdsupra.com/legalnews/europe-eu-commissioner-reding-introduc-85150/
45. Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J. and Bots, P. (2010) Policy Analysis of Multi-Actor Systems
46. European Commission (2012) Proposal for a regulation of the European parliament and of the Council щп the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Доступно через: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
47. CIGI-IPSOS Global Survey on Internet Security and Trust. Доступно через https://www.cigionline.org/internet-survey
48. Gavison, R., (1980) Privacy and the Limits of Law, Yale Law Journal 1980, vol. 89, p. 421, 428–436
49. Greenleaf, G. (2011) Global Data Privacy in a Networked World. Доступно через: http://ssrn.com/abstract=1954296

50. Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf
51. International chamber of commerce (2008) Privacy and Personal Data. Доступно через: http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/digitaleconomy/privacy-and-personal-data-protection
52. International Principles on the Application of Human Rights to Communications Surveillance. Доступно через: https://en.necessaryandproportionate.org/
53. International Working Group on Data Protection in Telecommunications. Доступно через: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt
54. ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» Доступно через: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en
55. ISO 22307:2008 on Financial Services: Privacy Impact Assessment (ISO 22307:2008 Финансовые услуги. Оценка влияния конфиденциальности)
56. OECD documents. Privacy and data protection: Issues and Challenges. Paris, 1966.
57. Raab, Ch. (1999) Governing Privacy: Systems, Participants and Policy Instruments// Proceedings of Ethicomp99: Fifth International Conference, Rome, 1999
58. Raab, C., Koops, B-J (2009), 'Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.edu
59. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) доступна по адресу: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
60. Rule, J.et al. (1980) The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York: Elsevier
61. Sadilek, A., Krumm, J.(2012) Far Out: Predicting Long-Term Human Mobility. Доступно через: http://www.cs.rochester.edu/~sadilek/publications/Sadilek-Krumm_Far-Out_AAAI-12.pdf
62. Schoeman, F. (1984) Philosophical Dimensions of Privacy: An Anthology. Доступно через: http://books.google.by/books/about/Philosophical_Dimensions_of_Privacy.html?id=q_FrmXyl3hUC&redir_esc=y
63. Schoeman, F. (1992) Privacy and Social Freedom. Cambridge, U.K.: Cambridge University Press.
64. Tan J (2008) A comparative study of the APEC privacy framework: A new voice in the data protection dialogue?. In Asian Journal of Comparative Law, 3(1). http://www.degruyter.com/dg/viewarticle/j$002fasjcl.2008.3.1$002fasjcl.2008.3.1.1071$002fasjcl.2008.3.1.1071.xml;jsessionid=F36717919BBF04391AC61CF44A516545
65. The Standard of Good Practice for Information Security, Information Security Forum (2003). Доступно через: http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf
66. Tucker, P. (2013) Has Big Data Made Anonymity Impossible?.Доступно через: http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible
67. 2B Advice (2012) Data Protection Practice 2012. Доступно через: https://www.2b-advice.com/GmbH-en/Study-Data-Protection-Practice-2012

БИБЛИОГРАФИЯ

68. Warren, S.D. and Brandeis, L.D., (1890) The Right to Privacy. Доступно через: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
69. Westin, A. (2003) Social and Political Dimensions of Privacy. Доступно через: http://www.asc.upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf
70. Westin, A. (1967) Privacy and Freedom. Доступно через: http://www.jstor.org/
71. Winn, J. (2008) Technical Standards as Data Protection Regulation. Доступно через: http://dx.doi.org/10.2139/ssrn.1118542